Spring 2-2013

E-Government Security in Municipal Government: A Case Study of Municipalities in Orange County, California

Timothy J. Perez

E-GOVERNMENT SECURITY IN MUNICIPAL GOVERNMENT: A CASE STUDY OF MUNICIPALITIES IN ORANGE COUNTY, CALIFORNIA

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Science

in

Information Systems

February, 2013

By
Timothy J. Perez, M.S., B.S.

Dissertation Committee:

Josh Pauli, Ph.D.
Surendra Sarnikar, Ph.D.
Mark Hawkes, Ph.D.

DAKOTA STATE
dsu
UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Science in Information Systems degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Timothy Perez

Dissertation Title: "E-Government Security in Municipal Government: A Case Study of Municipalities in Orange County, California

Dissertation Chair: ________ Date: 5/22/13

Committee member: Surendra Sarnikar Date: 5/22/13

Committee member: Mark Hawkes Date: 5/22/13

Committee member: ________ Date: ________

5/22/2013

ACKNOWLEDGMENT

I dedicate this work with great appreciation to my wife of over five years who without her continued support and encouragement this undertaking would not have been possible. I am truly thankful for her encouragement through the long evenings and nights preparing this work. Her understanding when we were unable to go out so that I could complete coursework, review lecture materials, gather research or write my dissertation. Her caring spirit allowed me to endure and persevere. Thank you from the bottom of my heart for everything!

I am also thankful to the extended support provided by my parents, family and friends throughout the course of my doctoral program. All of whom on occasion I was not able to accept many invitations due to my need to study and work on my doctoral program requirements.

Additionally, I am thoroughly impressed and appreciative of the support and guidance provided by the faculty of Dakota State University. In particular, I am wholeheartedly grateful for the guidance provided by my dissertation chair, Dr. Josh Pauli and my committee members throughout the entire dissertation process. Their feedback, guidance and direction were instrumental in reaching this important milestone.

ABSTRACT

Ample amount of evidence is available discussing the barriers to e-government adoption and initiatives. Of the many barriers or challenges mentioned, security concerns are a recurring theme (Angelopoulos, Kitsios, Kofakis, & Papadopoulos, 2010; W. A. Conklin, 2007; Ebrahim & Irani, 2005b; Gilbert, Balestrini, & Littleboy, 2004; Pipe, 2006; Schwester, 2009; Stibbe, 2005).

The majority of research however does not focus or discuss security considerations for e-government systems. This is even more notorious when looking specifically at municipal e-government literature. As such, this study takes an in-depth look at the e-government security practices of the 34 incorporated cities within the county of Orange, California through a descriptive case study. This case study yields important findings about the capabilities of municipal government agencies in implementing and maintaining secure e-government services by using federal e-government security requirements as a benchmark.

This study utilized a case study research design collecting both quantitative and qualitative data from the participating municipal agencies. To date, limited research has been conducted in the area of municipal e-government research as evidenced by the literature review conducted as part of this study.

Furthermore, this study proposed and responded to three (3) key research questions as follows:

1) What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?
2) How can municipal agencies reach a federal level of e-government security?
3) Why are municipalities not fully compliant with federal e-government security requirements?

To collect evidence this study asked all participants to complete a pre-interview participant survey. Subsequently, participants were interviewed and asked to respond to two interview questions. Findings from the survey indicate that average compliance with federal e-government security requirements as required by NIST SP800-44 was 38.05 percent as a totaled average. Participants were also asked to rate the degree of difficult in becoming fully compliant as easy, medium and difficult. The averaged totals for all 34 surveyed agencies were as follows: 20.59 percent (easy), 20.77 percent (medium) and 18.57 percent (difficult).

Results from the first participant interview question after coding yield seven (7) themes as to what the greatest challenges are to implementing and maintaining e-government security:

1) Staffing
2) Budget/Financial
3) Training/Expertise
4) IT Contract Services
5) Vendors
6) Changing Nature of IT Security
7) Time/Resources to Monitor Security Threats

Results from the second interview participant interview question in regards to what change or resource would assist municipal agencies in enhancing their e-government security were as follows:

1) Budgeting
2) Staffing
3) IT security training

Overall, the findings from this study highlight two key issues that surround municipal e-government security. First it is evident that from the surveyed agencies, compliance with all federal e-government security requirements does not exist. Secondly, municipal agencies needed additional resources in the forms of budget, staffing and training to be able to provide a federal level of e-government security.

DECLARATION

I hereby certify that this project constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the project describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Timothy J. Perez

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Introduction to the Problem

Electronic government or e-government is not a new topic, but is one of high interest to both the information systems and public administration research communities. From a business perspective organizations realize that in order to maintain a competitive edge and reduce costs technology must be leveraged to its fullest to streamline business operations (Eyob, 2004; Marchionini, Samet, & Brandt, 2003). As such, organizations now put themselves in greater contact with their customers through corporate websites, portals and integrated voice response (IVR) systems among others (Fiedler & Schmidt, 2005; Ho, 2002). This exposure subjects organizations to greater probabilities of security breaches and places an additional need to focus on the security of such systems (Choudrie, Raza, & Olla, 2009; Dutton, Guerra, Zizzo, & Peltu, 2005).

The trend to incorporate online services to enhance accessibility and reduce overhead costs has prompted the growth of e-government services in government agencies of all sizes. Although typically criticized for their inefficient and slow adoption of technology, government entities have employed such systems to provide better service to their constituents (Hazlett & Hill., 2003; Iglesias, 2010; Jun & Weare, 2008). This can be seen at all levels of government: federal, state and local. At the federal level, agencies such as the Internal Revenue Service (IRS) utilize e-government services to allow taxpayers to check the status of their refunds, apply for an employer identification number (EIN) and pay taxes online among other services. At the state level, the California Department of Motors Vehicles (DMV) provides for online vehicle registration and online booking of DMV appointments. Local municipalities are no exception either. Many cities provide several online services to their residents for items such as: filing noise complaints, code enforcement violations and paying business license taxes (Hofmann & Heierhoff, 2012; Jun & Weare, 2008). The collection of online services provided by government is typically referred to as electronic government or e-government. The type of e-government services provided by government agencies vary from locality and the level of government offering the service. Nonetheless, the trend can be seen that government entities are aware of the versatility and practicality of implementing online services to serve the public community (Gefen, Warkentin, Pavlou, & Rose, 2002; Scherlis & Eisenberg, 2003). Citizens enjoy the ability of being empowered with the capacity to perform various governmental activities without having to leave the comfort of their homes. This avoids long lines and hold times on the telephone to speak to government representatives (E. W. Welch, Hinnant, & Moon, 2005). At a first glance, all these e-government services seem like a win-win for both government and citizens.

However, this enhanced exposure also increases the security risks for agencies and especially for those utilizing or planning to adopt e-government services (M. M. Brown, 2000). The increase in identify theft, terrorist attacks and security breaches has emphasized the importance of information security (Li, 2011; Marques, Dias, & Zuquete, 2009; Taylor, 2002). In 2011 the police department's website for the City of Fullerton, California was a subject of numerous hacking threats from the hacking group known as Anonymous (Koerkner, 2011). In 2012, the city of Springfield, Missouri was also targeted by the Anonymous hacking group resulting in the personal information of over 2,100 users of the city's public website to be compromised (Penprase, 2012). As one would expect, the larger government agencies (federal and state) are subject to more regulation and oversight to safeguard citizens' personal and confidential information. However, municipal government agencies have very little regulation in regards to their e-government offerings. In most instances, if such security requirements do exist, these are frequently self-imposed.

In addition many municipal or local government entities simply do not have the resources to support and maintain secure e-government services. Municipal agencies, however gather information which should be treated with the same degree of confidentially and privacy as their larger federal and state counterparts. Thus, it is necessary for additional research in this area to determine the degree to which this problem exists.

Background of the Study

E-government is an emerging field with multidisciplinary interest. However, much of the existing literature in the realm of e-government discusses topics not directly related to security. For example, early research in e-government focused on taxonomies, models for adoption, and longitudinal studies of the impact of e-government on citizen satisfaction and trust (Beynon-Davies, 2007; Cohen, 2006; Dae-Ho Byun, 2011; Halaris, Magoutas, Papadomichelaki, & Mentzas, 2007; Hsu, Lin, Fang, & Chiu, 2012; Lee, Lee, & Kim, 2012). Recent literature has cited security as a common barrier or obstacle to adopting and maintaining e-government services (Angelopoulos et al., 2010; Baker & Bellordre, 2004; W. A. Conklin, 2007; Ebrahim & Irani, 2005b; Gilbert et al., 2004; Pipe, 2006; Schwester, 2009).

Of particular interest to this study is the United States E-Government Act of 2002. This key piece of legislation has had a significant impact on the role and usage of e-government services at the federal level in the United States (Levack, 2003). Title III of the E-Government Act of 2002 known more commonly as the Federal Information Security Management Act (FISMA) provides security requirements for federal agencies employing e-government services. This study will focus on the "Security Protocols to Protect Information" as required by Section 207(f)(1)(b)(iv) of the E–Government Act of 2002.

Currently, only federal agencies are required to comply with the E-Government Act of 2002 and its provision to provide security protocols to protect information (Seifert & Relyea, 2007). State and municipal government agencies are not subject to this federal act. This case study uses the federal approach to e-government security as a benchmark that municipal agencies should seek to attain. Federal agencies can comply with the security requirements of the act by following the guidance set forth by the NIST SP800-44 document published by the National Institute of Standards and Technology (NIST) a recognized authority in publishing security guidelines, policies, standards and procedures.

The NIST SP800-44 publication provides a series of seven (7) security checklists that can be used to ensure that all aspects of the policy have been applied appropriately. For this case study, municipal agencies were benchmarked against the degree of compliance in each of these seven security checklists. Each city (municipality) within the county of Orange, California was used as part of the study. Each agency was asked to indicate if they were compliant with each of the key sub-categories from all seven checklists. If they were not compliant, the agency was asked to provide the degree of difficulty that would be expected to achieve compliance and rated as: easy, medium or difficult.

Following this initial poll an interview was conducted with a representative from the agency. In most instances this representative had primary responsibility and oversight over the organization's information technology and information systems. Two questions were presented to the interviewee in each which they were asked to comment of the e-government security practices of their agency and also provide insight into the resources that could help their organization provide improved security on their e-government services.

Statement of the Problem

An ample amount of evidence is available discussing the barriers to e-government adoption and initiatives. Of the many barriers or challenges mentioned, security concerns are a recurring theme (Angelopoulos et al., 2010; W. A. Conklin, 2007; Ebrahim & Irani, 2005b; Gilbert et al., 2004; Pipe, 2006; Schwester, 2009; Stibbe, 2005) (Kostresevic & Simic, 2011; Luna-Reyes & Gil-Garcia, 2003; McLeod Jr. & Pippin, 2009; Paolo, Massacci, & Zannone, 2007; Stibbe, 2005).

The majority of research however does not focus or discuss security considerations for e-government systems. This is even more notorious when looking specifically at municipal e-government literature. As such, this study takes an in-depth look at the e-government security practices of the 34 incorporated cities within the county of Orange, California through a descriptive case study. This case study yields important findings about the capabilities of municipal government agencies in implementing and maintaining secure e-government services by using federal e-government security requirements as a benchmark.

Purpose of the Study

The purpose of this study was to explore and further understand the e-government security capabilities and practices of municipal government. This study utilized a case study research design collecting both quantitative and qualitative data from the participating municipal agencies. To date, limited research has been conducted in the area of municipal e-government research as evidenced by the literature review conducted as part of this study.

This shed light on the information security practices and resources of municipal government entities through a descriptive case study of municipalities within Orange County, California. The County of Orange is home to 34 incorporated cities of varying size and demographics. This county provides an adequate spread between cities which allowed the findings and contributions of this research to be applicable in other instances.

Research Questions

This research project and study addresses three (3) key research questions as follows:

1) What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?
2) How can municipal agencies reach a federal level of e-government security?
3) Why are municipalities not fully compliant with federal e-government security requirements?

Significance of the Study

This research project analyzed municipal e-government security through the lens of the E-Government Act of 2002 and specifically the key provision directly relating to federal e-government security: Security Protocols to Protect Information

It is important to note however, that municipal government agencies are not required to adhere to these security requirements. At the moment, the requirements of the E-Government Act of 2002 apply only federal agencies. Nonetheless, the research project investigated which of these requirements municipal government entities were compliant with and how they could become more compliant.

Assumptions and Limitations

Assumptions

For this study one key assumption that has been made is that all participants answered honestly to all questions. Each participant from the case study was first asked to independently respond to a set of questions that provided information regarding their municipality along with their compliance or ability to comply with the various requirements of the NIST SP 800-44 Security Checklists. Each participant was then interviewed and asked two questions. It is the assumption of this study that each participant answered all questions in an honest manner.

It is further assumed that each of the participants of this study fully understood and comprehended each of the questions that were asked of them. During both phases (independent responses to questions and interview) the participants were provided with the opportunity to ask for clarification or guidance on any item. No participant asked for follow-up explanations, so it is thereby assumed that all participants fully understood all aspects of the questions they was presented.

Limitations

This study noted certain limitations and also defined the research scope. This case study is limited to the incorporated municipalities within the county of Orange, California. No county or state agencies were included as part of this study. Orange County has a reasonable spread of municipal agencies with varied financial resources and demographic backgrounds. While many of the conclusions that have been developed as a result of this study are applicable to other similar municipalities, should these findings be used in other research endeavors each researcher is responsible for confirming the degree to which these findings are applicable to their specific scenario.

Second, each participant was provided with a statement of confidentially and anonymity to help prevent any biased responses. However the possibility does exist that some responses may have been biased fearing negative repercussions from their superiors.

Third, this study was not designed to be the authoritative study on municipal government security. Instead it is an exploratory and descriptive study into municipal e-government security utilizing municipalities within Orange County, California as participants. Therefore, it is possible that other researchers can reach a different set of findings when looking at another municipal agency.

Lastly, while an exhaustive literature review and search was performed in preparing the results and findings of this study, it is possible that some findings or conclusions already existed without the researcher's knowledge. Nevertheless, this study provides a significant and unique look into municipal e-government security by means of a case study approach.

Nature of the Study

This research project utilized a descriptive case study research approach. The research focuses on understanding e-government within a municipal context to ascertain an improved understanding of how e-government is influenced by this context (M. Myers, 1997). As such this research study adopts a set of philosophical assumptions that are inherent of interpretive research.

A case study research approach was selected for this study as this research model is one frequently used in information systems research (Orlikowski & Baroudi, 1991). Furthermore, this study utilized the recommendations set forth by Walsham (1995) for interpretive case study research.

Organization of the Remainder of the Study

This dissertation is organized into five (5) chapters. This chapter serves as the introduction to the research project and study. It includes the introduction to the problem, the background of the study, the statement of the problem, the purpose of the study, the research questions, the significance of the study, the assumptions and limitations of the study, and the nature of the study.

Chapter 2 provides a literature review of pertinent literature and is subdivided into smaller sections by topic.

Chapter 3 describes the research methodology and design that was utilized for the study.

Chapter 4 includes the data collected for the study, a summary of findings and the relevant data analysis that was conducted.

Chapter 5 discussed the contributions of the study, provides suggestions for future discussion and furnishes the concluding remarks of the study.

CHAPTER 2

LITERATURE REVIEW

Overview of E-Government

In gathering information for this research project an extensive literature search and review has taken place. As a primary resource, the E-Government Reference Library (EGRL) version 8.5 was utilized. The EGRL is a comprehensive bibliography of e-government publications maintained by the iSchool at the University of Washington. E-Government continues to remain a topic of heighten research interest with over 850 new peer-reviewed publications in the English language being added to the EGRL in its last revision. The EGRL currently contains over 5,524 bibliographic references from a variety of peer-reviewed outlets including journals, conferences, books and other sources.

The table below highlights the number of publications within the EGRL that are specific to local, municipal or city government.

Table 2.1: Number of Local E-Government Sources in the EGRL

Keyword	Number of Sources	Percentage of Total EGRL Library*
City	59	1.07%
Municipal	97	1.76%
Local	274	4.96%
Total	**430**	**7.78%**

*Total number of literary sources in the EGRL = 5,524

In addition to the literature sources identified above, other sources within the library were identified. The abstracts or overviews were reviewed to determine their applicability to the topic. The following criteria were used to determine the applicability for the purposes of this study:

1) Research paper had a primary focus of e-government

2) Focused on the use, implementation or effects of e-government
3) Excluded papers having a primary focus of e-voting systems
4) Relevance to research topic

The literature search revealed that there is an even distribution of publications in the business related disciplines as compared to the publications in information systems related outlets. The publication of e-government information in different disciplines suggests that the topic is multi-dimensional and is of interest to multiple research fields. It also illustrates the need to analyze a given research topic using the tools from different disciplines.

Recent reports on e-government initiatives show a growing trend among all levels of government. It is estimated that at the federal level only, the United States spent in excess of $2 billion in 2006 for e-government related activities (Belanger & Hiller, 2006). Adoption of new technologies and strategies to enhance government activities in the online arena are present at virtually all levels of government. Publication of e-government research has occurred in both the public administration and information systems outlets. Although most articles are broad in nature and typically deal with more theoretical and managerial implications of e-government, the literature search concluded in the following seven themes that were prevalent among extant e-government publications:

1. **e-Government Frameworks**: (Apostolou, Mentzas, Stojanovic, Thoenssen, & Lobo, 2011; Belanger & Hiller, 2006; Chutimaskul, Funilkul, & Chongsuphajaisiddhi, 2008; Cordella & Iannacci, 2010; Crichton, Davies, Gibbons, Harris, & Shukla, 2007; S. Dawes, 2008; Gupta & Jana, 2003; Nour, AbdelRahman, & Fadlalla, 2008; Raus, Liu, & Kipp, 2010; Sarantis, Charalabidis, & Askounis, 2011)
2. **Classifications of e-Government**: (Arabatzis, Andreopoulou, Koutroumanidis, & Manos, 2010; Gupta & Jana, 2003; Halaris et al., 2007; Layne & Lee, 2001; Lee et al., 2012; Mosse & Whitley, 2009; Olbrich, 2010; Zhou, 2008)
3. **Types of services offered**: (Gil-Garcia & Martinez-Moyano, 2007; Gupta & Jana, 2003; Kaaya, 2009)
4. **Legislation concerning e-Government**: (Alpar & Olbrich, 2005; Basu, 2007; Brunschwig, 2002; Chissick, Harrington, & Azhar, 2004; Gil-Garcia & Martinez-

Moyano, 2007; Kiskis & Petrauskas, 2003; Paolo et al., 2007; Saarenpää, 2003; Taylor, 2002; Wilson, 2012)

5. **Common barriers to e-Government**: (Angelopoulos et al., 2010; Archmann & Nielsen, 2008; Ayyad, 2009; Baker & Bellordre, 2004; W. Conklin, 2007; W. A. Conklin, 2007; Ernani Marques dos Santos & Reinhard, 2010; E. M. dos Santos & Reinhard, 2012; Ebrahim & Irani, 2005a, 2005b; Faisal & Rahman, 2008; Lam, 2005; Pipe, 2006; Schwester, 2009; van Veenstra, Klievink, & Janssen, 2009)
6. **Citizens' trust and confidence in e-Government**: (Akkaya, Wolf, & Krcmar, 2010; Al-Sobhi, Weerakkody, & El-Haddadeh, 2012; S. A. Becker, 2005; Bélanger & Carter, 2008; Carter & Bélanger, 2005a, 2005b; Choudrie et al., 2009; Dutton et al., 2005; Galindo, 2002; Horsburgh, Goldfinch, & Gauld, 2011; Huijboom & Hoogwout, 2004; McLeod Jr. & Pippin, 2009; Navarrete, 2010; M. Parent, C. Vandebeek, & A. Gemino, 2005; M. Parent, C. A. Vandebeek, & A. C. Gemino, 2005; Richards, Adam, & Price, 2005; Rowe, 2007; Smith, 2010; C. Tolbert & Mossberger, 2003; C. J. Tolbert & Mossberger, 2006; E. W. Welch et al., 2005; Yee et al., 2005)
7. **Security concerns of e-Government solutions**: (J. Becker, Hofmann, & Räckers, 2011; Berghmans & Van Roy, 2011; Brechbuhl, 2010; Y.-S. Chen, Chong, & Zhang, 2004; A. Conklin & G. White, 2006; A. Conklin & G. B. White, 2006; Hof, 2003; James B. D. Joshi, Ghafoor, Aref, & Spafford, 2002; James B.D. Joshi, Joshi, & Chandran, 2007; Kjaerland, 2006; Levack, 2003; Luna-Reyes & Gil-Garcia, 2003; McLeod Jr. & Pippin, 2009; Si & Li, 2007; Stibbe, 2005; Wang, 2009; Wimmer & von Bredow, 2002; Winkel, 2007; Zhao & Zhao, 2010)

A principle question that arises when dealing with e-government is how to define what e-government is and what it encompasses. In comparison to other more established research topics, e-government is still considered relatively new (Grant & Chau, 2005). As such, some scholars disagree as to what services should fall under the umbrella of e-government. As is commonly seen in research the definition of a given phenomenon can vary depending on the perspective used by the person providing such a definition.

In defining e-government (Scholl, 2003) describes this as "the use of information technology to support operations, engage citizens, and provide government services" (Scholl, p. 2). Under this term, just about any information technology (IT) system used to support and engage citizens could thereby be considered an e-government system. However, e-government is not typically thought of the computer and servers used to by government employees to provide citizens with information. Instead it is more commonly considered the self-support or online services provided by government (Carter & Bélanger, 2005b). These services support and enhance government efficiency when interacting with citizens.

Regardless of the various viewpoints on the definition of e-government, the majority of scholars agree that one key goal or output of e-government is improved efficiency (Eyob, 2004; Grönlund, 2002; Thomson, 2011). In looking at the gradual evolution of government technology, efficiency has always been an important motivating factor towards adopting such systems. For example, technology in many government offices was seen in the early 1970s when many government agencies adopted mainframe computer systems to automate routine processes and calculations. Later, in the 1980s the microcomputer was smaller and more affordable. This allowed government agencies to use some systems for information and data processing.

The 1990s were a time when many government agencies adopted large scale enterprise resource planning (ERP) systems which automated payroll, accounting, budgeting and other common tasks. Around the late 90s and at the turn of the millennium many agencies moved to the Internet to offer online services (Relyea & Hogue, 2004). Just as businesses learned the value of the Internet so did government agencies. Beginning in the late 90s many government agencies including municipalities throughout the United States launched their first websites (Grönlund & Horan, 2005).

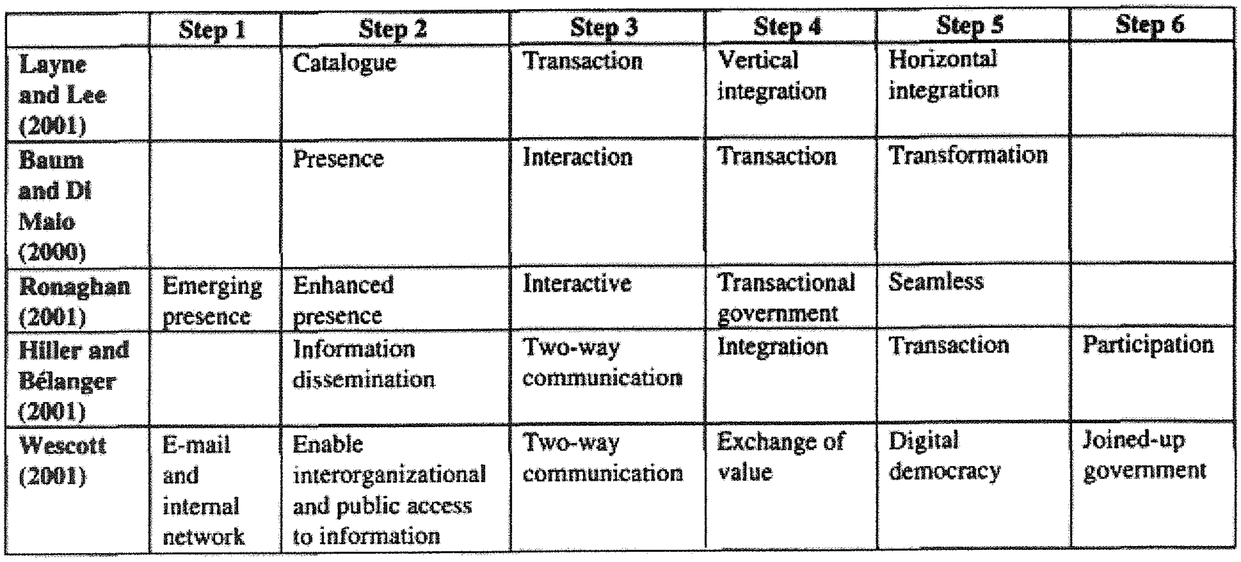
Today, e-government is considered the collection of online and web services offered to interact with citizens, businesses and even other government agencies (Gil-Garcia & Luna-Reyes, 2003; Wyld, 2004). E-government services are adopted by agencies for a wide variety of reasons. Some agencies are mandated to do so, others capitalize on the cost savings produced by enhanced efficiency and others do so to better serve their citizen base. The unique nature of each government agency adds to the complexity in defining and specifying requirements for a particular initiative. Overall however, e-government serves as a necessary component in the IT portfolio of most government agencies today.

E-Government Models

E-government systems can be highly complex and differ from one another. However, modeling e-government systems provides a method to more easily understand and research these services. The intricacy of e-government is described by some with a three stage model comprised of: initiation, infusion and customization. Yet others utilize another that focuses on communication as: one-way communication, two-way communication, exchanges and portals (Belanger & Hiller, 2006).

Early works in the 2000s provided for several models for e-government. Many of them classified e-government based on the degree of adoption or the technological advancements of the organization. The figure below highlights common model stages as identified by (Coursey & Norris, 2008).

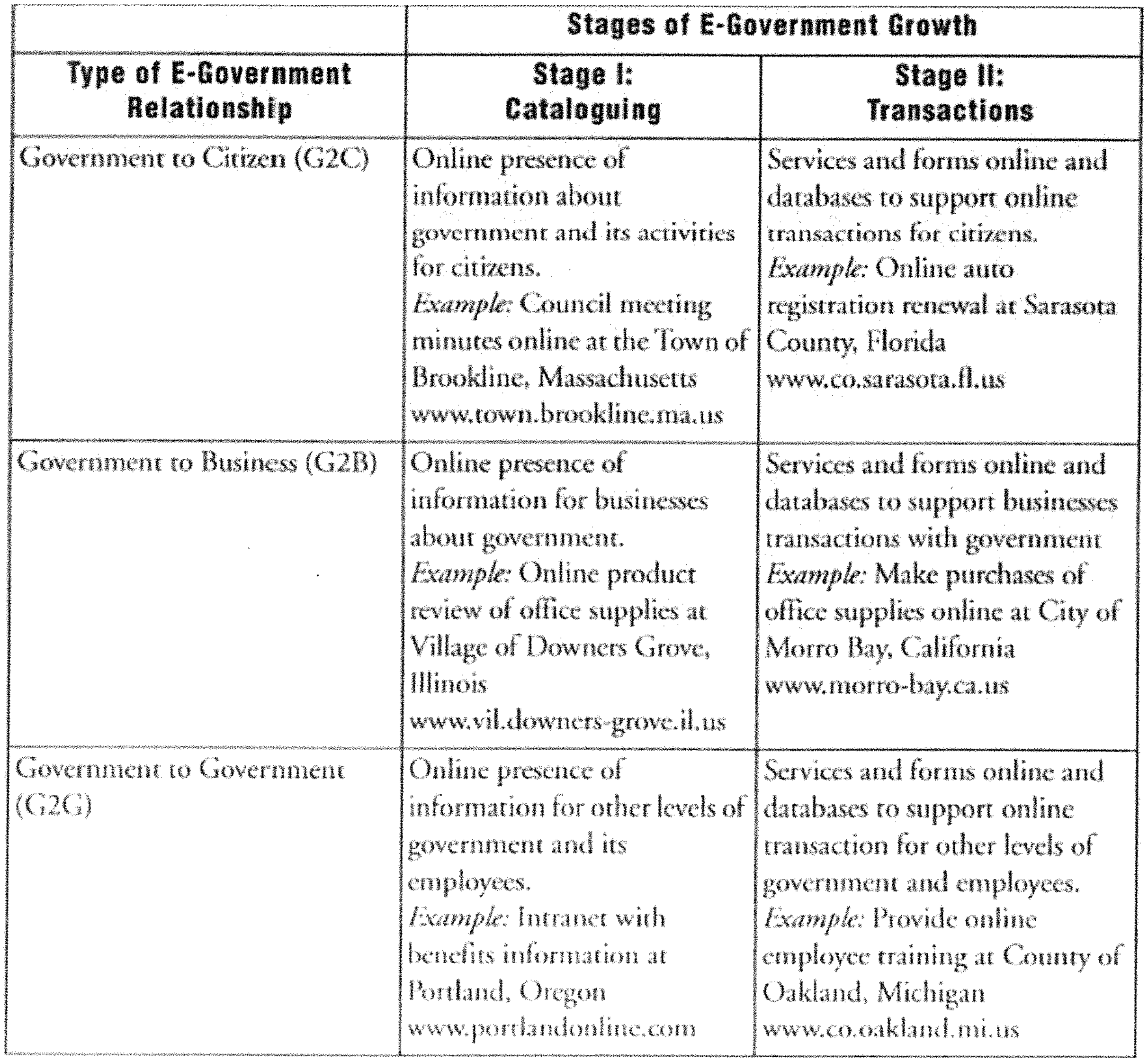
Figure 2.1: E-Government Models (Coursey & Norris, 2008)



	Step 1	**Step 2**	**Step 3**	**Step 4**	**Step 5**	**Step 6**
Layne and Lee (2001)		Catalogue	Transaction	Vertical integration	Horizontal integration	
Baum and Di Maio (2000)		Presence	Interaction	Transaction	Transformation	
Ronaghan (2001)	Emerging presence	Enhanced presence	Interactive	Transactional government	Seamless	
Hiller and Bélanger (2001)		Information dissemination	Two-way communication	Integration	Transaction	Participation
Wescott (2001)	E-mail and internal network	Enable interorganizational and public access to information	Two-way communication	Exchange of value	Digital democracy	Joined-up government

Others when classifying e-government compare it to the more established discipline of e-commerce. When describing e-commerce transactions it is common to mention terms such as business-to-customer (B2C), business-to-business (B2B), business-to-employee (B2E) and customer-to-business (C2B). Similarly, e-government transactions can also be described in this same context as: government-to-citizen (G2C), government-to-employee (G2E) and government-to-government (G2G) (Moon & Norris, 2005). In this context, one can see that government can interact with citizens, employees, and even other governmental institutions in a comparative fashion as e-commerce (Carter & Bélanger, 2005a). In correlating e-government to its growth, Reddick also uses the classifications of G2C, G2B and G2B (Reddick, 2005). The Figure 2.2 below highlights Reddick's representation of transactions that occur within each type of e-government classification.

Figure 2.2: Stages of E-Government Growth (Reddick, 2005)



	Stages of E-Government Growth	
Type of E-Government Relationship	**Stage I: Cataloguing**	**Stage II: Transactions**
Government to Citizen (G2C)	Online presence of information about government and its activities for citizens. *Example:* Council meeting minutes online at the Town of Brookline, Massachusetts www.town.brookline.ma.us	Services and forms online and databases to support online transactions for citizens. *Example:* Online auto registration renewal at Sarasota County, Florida www.co.sarasota.fl.us
Government to Business (G2B)	Online presence of information for businesses about government. *Example:* Online product review of office supplies at Village of Downers Grove, Illinois www.vil.downers-grove.il.us	Services and forms online and databases to support businesses transactions with government *Example:* Make purchases of office supplies online at City of Morro Bay, California www.morro-bay.ca.us
Government to Government (G2G)	Online presence of information for other levels of government and its employees. *Example:* Intranet with benefits information at Portland, Oregon www.portlandonline.com	Services and forms online and databases to support online transaction for other levels of government and employees. *Example:* Provide online employee training at County of Oakland, Michigan www.co.oakland.mi.us

Comparing e-government to e-commerce is a well suited match. The field of e-commerce is more mature, developed and researched. Yet, e-government can truly be said to be nothing more than government agencies using the same online and web technologies that business have been using for much longer. Other researchers have suggested that e-government can learn many valuable lessons from its e-commerce counterpart (Scholl, 2006). Thus comparing e-government to e-commerce can broaden the understanding of online technology and adoption by governmental organizations.

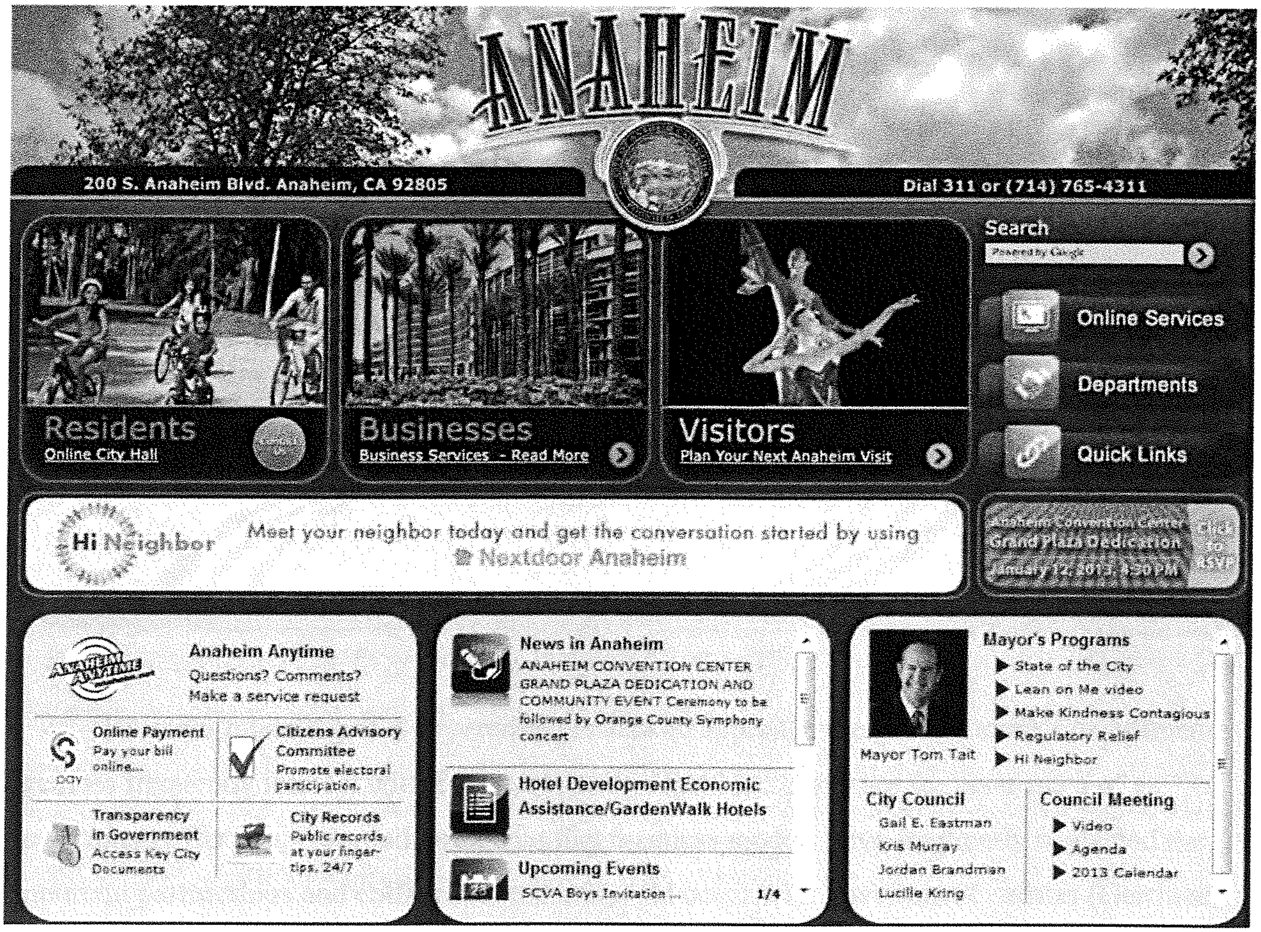
Another stance on modeling e-government is provided by Moon who classifies e-government transactions into two distinct categories: financial and non-financial transactions (2005). Financial transactions typically include activities such as: paying for taxes, fines, licenses, utilities and citations. However, the larger list was comprised of non-financial transactions which included items such as: services requests, records requests/searches, maps, permit renewals, program registration and communication with elected officials. This evidence clearly demonstrates a trend in utilizing e-government for a growing number of services.

Moon's distinction between financial and non-financial transactions is an important one. Financial related transactions carry higher-level of security and confidentially than that of non-financial inquires. Providing this distinction early on can allows for enhanced security provisions for those transactions that are considered financial. Other researchers have also suggested that when payment systems are involved a separate model should be utilized (Wittmann, Breitschaft, Krabichler, & Stahl, 2007). Using a separate model for this aspect would account for the intricate details that should be addressed as part of e-government offerings including payment functionality.

Other researchers have taken a holistic approach on e-government suggesting that it should be an all-inclusive or one-stop solution. In larger government agencies it is not uncommon to see e-government services spread out amongst various web pages or websites. This approach however, can make it difficult to quickly locate all the online e-government services provided by an agency. Glassey suggests that one-stop models to e-government have been very effective in European countries and that similar approaches should also be explored for agencies within the United States (Glassey, 2004).

Of the cities included in the part of this study, the City of Anaheim, California provides a good example of how municipal government agencies can utilize the one-stop e-government model. Figure 2.3 shown below highlights how this organization consolidated all of their online (e-government) services on their homepage and makes them available through a single button titled "Online Services".

Figure 2.3 – City of Anaheim Homepage


ANAHEIM
200 S. Anaheim Blvd. Anaheim, CA 92805
Dial 311 or (714) 765-4311
Residents
Online City Hall
Businesses
Business Services - Read More
Visitors
Plan Your Next Anaheim Visit
Search
Powered by Google
Online Services
Departments
Quick Links
Hi Neighbor
Anaheim Convention Center Grand Plaza Dedication January 12, 2013, 4:30 PM
Click to RSVP
Anaheim Anytime

Meet your neighbor today and get the conversation started by using Nextdoor Anaheim

Anaheim Anytime
Questions? Comments?
Make a service request

Online Payment
Pay your bill online...

Citizens Advisory Committee
Promote electoral participation.

Transparency in Government
Access Key City Documents

City Records
Public records, at your finger-tips. 24/7

News in Anaheim
ANAHEIM CONVENTION CENTER GRAND PLAZA DEDICATION AND COMMUNITY EVENT Ceremony to be followed by Orange County Symphony concert

Hotel Development Economic Assistance/GardenWalk Hotels

Upcoming Events
SCVA Boys Invitation ... 1/4

Mayor Tom Tait

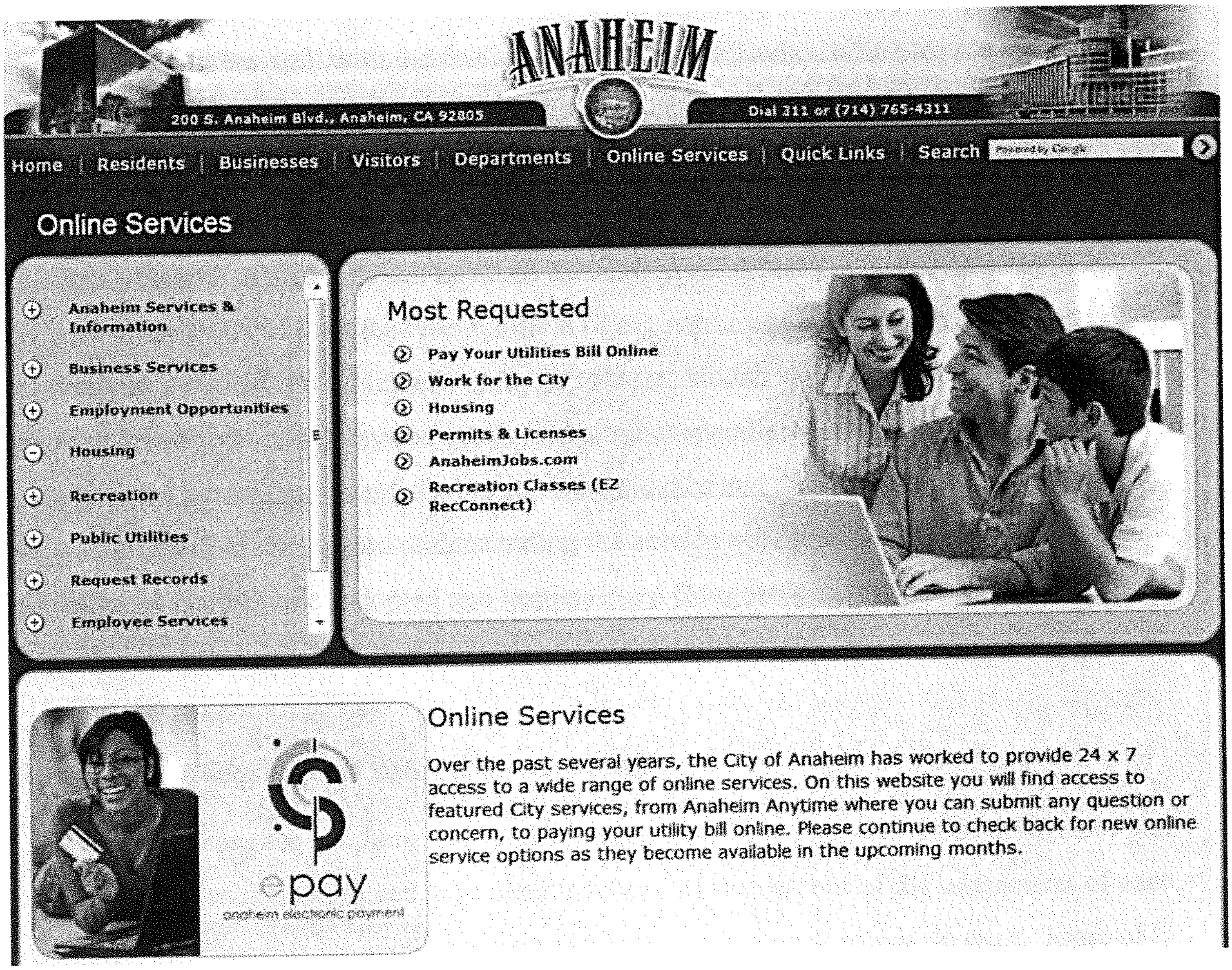
Mayor's Programs
▶ State of the City
▶ Lean on Me video
▶ Make Kindness Contagious
▶ Regulatory Relief
▶ Hi Neighbor

City Council
Gail E. Eastman
Kris Murray
Jordan Brandman
Lucille Kring

Council Meeting
▶ Video
▶ Agenda
▶ 2013 Calendar

Subsequently, figure 2.4 illustrates the online services section of the City of Anaheim website. Using this approach allows citizens viewing the website to access all of the agency's e-government resources in a single page. The cities included in this study utilized various approaches to organizing and collecting their e-government offerings. Some, like the Anaheim gathered them all in a single location. Others required that the user navigate to the section or department page to access the e-government services for that given category.

Figure 2.4 – City of Anaheim Online Services Section


ANAHEIM
200 S. Anaheim Blvd., Anaheim, CA 92805
Dial 311 or (714) 765-4311
Home | Residents | Businesses | Visitors | Departments | Online Services | Quick Links | Search
Powered by Google
Online Services
Anaheim Services & Information
Business Services
Employment Opportunities
Housing
Recreation
Public Utilities
Request Records
Employee Services
Most Requested
Pay Your Utilities Bill Online
Work for the City
Housing
Permits & Licenses
AnaheimJobs.com
Recreation Classes (EZ RecConnect)
epay
anaheim electronic payment

Online Services

Over the past several years, the City of Anaheim has worked to provide 24 x 7 access to a wide range of online services. On this website you will find access to featured City services, from Anaheim Anytime where you can submit any question or concern, to paying your utility bill online. Please continue to check back for new online service options as they become available in the upcoming months.

Business modeling of e-government is also an approach seen in literature. Government agencies frequently interact with businesses and in fact businesses are frequent users of e-government offerings. Gertraud points out that business models have frequently neglected the important partnerships and collaboration that should occur with government entities (Gertraud Peinel, 2010). Thus, Gertraud recommends and proposes various approaches to modeling e-government services so that they align with the needs of businesses. Other researchers have also hinted at the importance of modeling e-government to recognize business needs (Janssen, Kuk, & Wagenaar, 2005; Joha & Janssen, 2011; Loukis & Tavlaki, 2007; Panagiotopoulos, Al-Debei, Fitzgerald, & Elliman, 2012).

Furthermore, by using a case study approach Yadav and Yadav recognize that an entirely new model is needed for e-government altogether (Yadav & Yadav, 2009). Many other models have focused on a specific aspect of the e-government process, implementation or usage. Yadav instead recommends a model that encompasses all aspects of e-government. This research agrees well with the findings of Loukis and Tavlaki who propose models for designing, supporting and maintaining public to private partnerships (Loukis & Tavlaki, 2007).

Overall, it is evident that e-government in itself is a complex phenomenon and that different research approaches can be taken to classify, model and interpret these services (Beynon-Davies, 2007). As the research field of e-government continues to mature so will the models and definitions used in delimiting its context. Models that may apply or be useful in one scenario, might not always be applicable in other specific instances (Coursey & Norris, 2008). These models are established to furnish guidance and direction. New literature also shows a trend to modeling and understanding the service quality and reliability of e-government systems once adopted and implemented (Magoutas & Mentzas, 2009). In all, each model presents its own set of advantages and disadvantages.

Reasons for Adopting and Using E-Government

The reasons for adopting and implementing e-government services are as diverse and complex as the models designed to understand them. However, out of the uniqueness of each given agency's impetus for adopting e-government, some general trends do exist. Some of these include the desire to enhance organizational efficiency, reduce overhead or administrative processing costs, develop an improved sense of openness and trust, and providing enhanced convenience to a government agency's constituents.

Much has been published on efficiency as a motivating factor for adopting e-government (Chourabi, Mellouli, & Bouslama, 2009; Eyob, 2004; Grönlund, 2002; Iglesias, 2010; Jun & Weare, 2008; Khayyat, 2010; Lee, Oh, & Kwon, 2008; Sell, Patokorpi, & Walden, 2006; Thomson, 2011; Yarlagadda & Ahmed, 2007). Many government agencies that have participated in business process remodeling (BPR) have found that incorporating e-government systems or technologies can help enhance their level of efficiency. In doing so some researchers suggest modeling e-government business process during the adoption phase to maximize the efficiency of such systems (Chourabi et al., 2009).

Increased organizational efficiency usually has a positive effect on citizen satisfaction. Some studies have suggested that efficiency and increased citizen satisfaction are two primary outputs of e-government systems (Ciborra, 2005). Efficiency is an important factor for government agencies because enhanced and streamlined operations frequently reduce overhead costs for government. Smaller government agencies as surveyed in this case study are usually more sensitive to budgetary changes that are a result of fluctuations in the economic climate. Augmenting efficiency for some has been a way to combat shrinking budgets by maximizing existing resources and staff.

For other agencies, a key motivating factor for e-government is reducing administrative and employee related costs. Depending the type of government entity and location some agencies still process a large variety of items in a manual fashion. As such, the lack of online services or automation results in the need for increased staffing and overhead. Adopting and using e-government systems has been cited by several researchers as a method to reduce the administrative burden that numerous government agencies face (Alessia C. Neuroni, 2010; Andersen & Medaglia, 2008; Arendsen & van Engers, 2004; Mary Maureen Brown, 2001; Decman & Klun, 2010; Eyob, 2007; Hadzilias, 2005).

Initiatives to enhance government transparency at the national level in the United States have spawn agencies at all levels to look for technologies to provide such citizen access. As a result, many local, state and federal agencies have adopted or enacted measures which require their organizations to provide openness and transparency to the public. To comply with these requirements some government agencies have adopted or enhanced their use of e-government services. Recent publications show that transparency is a concern and reason for utilizing e-government for agencies at all levels (Bertot, Jaeger, & Grimes, 2012; Bonsón, Torres, Royo, & Flores, 2012; X. Chen, Kong, & Futatsugi, 2007; Ciborra, 2005; S. S. Dawes & Helbig, 2010; Fenster, 2012; Grimmelikhuijsen, 2012; Helbig, Styrin, Canestraro, & Pardo, 2010; Ostermann & Staudinger, 2007; Piotrowski & Borry, 2009; Eric W. Welch & Hinnant, 2003; Zinnbauer, 2007).

For agencies concerned with enhancing the trust of their citizen base, e-government systems have proven helpful in this area as well. In most instances, increased levels of e-government have allowed citizens to have easier and faster access to government records and information. This enhanced access has reduced the perception of government corruption or inefficient spending (Ostermann & Staudinger, 2007; Roy, 2005; Eric W. Welch & Hinnant, 2003; Zinnbauer, 2007). Openness, transparency and trust are closely tied together and can all be supported by accessible e-government systems.

Convenience and increased accessibility is another factor for e-government adoption. Very few government agencies provide around-the-clock or 24-hour availability. By implementing e-government solutions, agencies can frequently provide 24-hour a-day availability. E-government is also beneficial to those with disabilities or with limited transportation (Fogli, Colosio, & Sacco, 2010). Online services can provide a method for those individuals to interact with government independent of time and place. As online services in other areas grow, citizens have increased expectations of online services from their government agencies. This convenience is considered by many as a "must" and no longer a luxury.

In general there are many reasons as to why government agencies employee e-government services. As described in this section there are many benefits and positive reasons to implement e-government solutions. Most agencies are impelled to implement a given e-government service for more than one reason. In one instance a combination of efficiency, increased access and reduced operating costs might lead one agency to adopt e-government. Yet others may choose a completely different set of items as their motivating factors. Nonetheless, regardless of the precise reasons for adoption, recent publications and reports show government agencies are adopting and enhancing their e-government offerings at a growing rate.

Barriers to Adopting E-Government

It is evident as described in the previous section that numerous reasons exist to adopt e-government solutions. However, despite the many benefits that e-government services offer, there are still many barriers and challenges that agencies face when attempting to adopt e-government systems. Even in those projects that resulted in a successful implementation and acceptance obstacles were stilled seen.

Information sharing among government agencies was a common theme prevalent among all levels of government. However, businesses utilizing e-commerce technologies were noted to typically shy away from information sharing as compared to the public sector

(Sharon L. Caudle, Gorr, & Newcomer, 1991). Yet, one of the key deterrents in information sharing in governments agencies is a byproduct of incompatible legacy systems. The larger the agency the harder it becomes to stay current with technology and modernize legacy systems (Stamoulis, Gouscos, Georgiadis, & Martakos, 2001). As such, e-government has also been implemented with the hopes of remedying this situation with the expectation that G2G transactions can be accomplished via such avenues despite more direct sharing methods.

Despite the obvious advantages of e-government not only for citizen communication but also for intergovernmental transactions, many barriers still exist. Barriers can typically be classified into the following three categories: political, financial or technological (Ebrahim & Irani, 2005a). Of particular interest are those that are technological in nature. In some instances, there is no existing platform to perform a customized e-government service and developing such a service would be too cost prohibitive. Other limitations reside not with the governmental institution, but on occasion with a given community's demographics as it relates to their access to technology. Naturally, implementing a service that would have little or no usage would not be well advised.

Another common but frequently overlooked facet is a citizen's trust in a certain agency (Akkaya, Obermeier, Wolf, & Krcmar, 2011; Akkaya et al., 2010; Carter & Bélanger, 2005a; Yee et al., 2005). The aspect of trust is not one that is centric just to a particular state or country. Instead, concerns of government trust and privacy in relation to e-government are seen at a global level (Das, DiRienzo, & Burbridge, 2009). Trust can implicate a given agency's reputation and past performance with the public. Or even more important, the lack of response from citizen initiated contacts from e-government services (Thomas & Streib, 2003). The perception that in-person contact will be more effective than online contact can have a devastating effect on a given e-government service. Research has shown that levels of trust in e-government are elevated with positive online responses and outcomes (LaVoy, 2001; Eric W. Welch, 2005; West, 2004). For that reason, government agencies should strive to ensure that online contact from citizens receives equal or greater support than contact from other traditional methods.

Of the various barriers mentioned, security seems to take a back seat (Norris & Moon, 2005). The paradox however, is that security is a growing concern amongst government agencies and their respective citizens (Taylor, 2002). Some agencies may just be too small to employ the necessary staff to address such issues, while others simply overlook the security concerns by highlighting the online service's features (Lee, Xin, & Trimi, 2005).

Larger agencies such as federal and state agencies typically provide for more thorough security measures because the likelihood of an attack is much greater. Unfortunately, many local government agencies fast-track security under the premise that such an investment is not necessary and therefore fail to implement proper security countermeasures. For this reason, many local cities and small government agencies have fallen victims to information breaches and other security threats. Research indicates that citizens are constantly becoming more "connected" by using computers, Internet, mobile phones and other forms of communication to stay in touch with their government agencies (Thomas & Streib, 2003). As such, a greater commitment to security is necessary from municipal government agencies.

One of the common barriers to implementing and adopting e-government solutions that was discussed earlier was "security". Public officials realize that e-government systems can place their entities at greater risk for terrorist or other malicious attacks (Halchin, 2004). A recent security assessment on the state of e-government websites found the creation of opportunities and threats. The solutions provided a wide variety of services to citizens, but also created a myriad of new threats (Zhao & Zhao, 2010).

Many methods exist to implement security for e-government. But in general e-government should address the three key areas of information security: confidentially, integrity and availability (McCumber, 2005). Integrity can be conserved by ensuring that an audit trail is maintained and that all changes or updates to the systems are documented (van Velsen, van der Geest, ter Hedde, & Derks, 2009). Additionally, security should be a primary concern and needs to be built into the system and not performed as an afterthought once the system has already been fully developed (Meneklis & Douligeris, 2010). Lastly, risks should also be identified and evaluated to protect any citizen information that has been collected (Bélanger & Carter, 2008).

The literature review found a large pool of e-government related publications. However, the majority of the articles lacked a security focus. Part of the reason for this is that half of such articles were published in business, management or public administration journals. As such, the articles focus on managerial issues and strategies for implementation. Others discussed barriers for implementations and frameworks to describe and classify such e-government initiatives (S. L. Caudle, 1990). The other half of publications were found in articles published in the information systems (IS) discipline. Unfortunately, even works published in IS conduits, failed to accurately address the need for security and especially at the municipal government level.

Security however, was not an unknown factor. Most articles touched on the topic of security, however not extensively enough to define a framework for addressing security implications of e-government. Instead, security was merely mentioned as a barrier or as a factor to consider when seeking to implement such a system (Moon & Norris, 2005). In many instances, security is often left last due to its intricate and complex application in the e-government arena. Although of extreme importance, management often seems to believe that security hurdles are the easiest to overcome (Mitrakas, Hengeveld, Polemi, & Gamper, 2007). For that reason, many initiatives often see delays. Security concerns are often not addressed and realized until the final steps of an implementation (Kaliontzoglou, Sklavos, Karantjias, & Polemi, 2005).

For these reasons this research project focuses on security. Researchers tend to focus on the larger federal and state agencies and often neglect the important role that local government plays in communities (Rice, Alsobrook, & Weinberger, 1982). As such, this case study seeks to understand the limitations of smaller municipal government agencies to understand how they can still achieve and maintain a reasonable degree of e-government security as compared to their federal counterparts.

E-Government at the Municipal Level

Municipal or local government agencies represent the smallest level of government in the United States. Since municipal government agencies are much smaller than their larger state and federal counterparts they have the ability to enjoy a more personal and intimate relationship with their citizen base. The needs and priorities for municipalities may differ greatly from that even of a neighboring city. Many municipal agencies have already established a degree of trust and understanding with their respective communities. This allows these agencies to be in the most opportune state to serve their population.

There are numerous reasons to implement, adopt and utilize e-government solutions and these also apply to municipal government. Municipal agencies can capitalize on the benefits of e-government in a similar fashion as state and federal agencies. Municipal government is typically the first point of contact for citizens and businesses within an assigned jurisdictional area. The intimate relationship between citizens and municipal agencies provides an excellent foundation to strengthened ties and business activities.

One such reason municipal agencies are primary points of contact for citizens is because they usually more accessible than larger state and federal agencies. Government was formed to support and assist the public community that it serves. E-government provides opportunities to enhance the service provided to citizens and improve the overall customer experience. Andresen points out that online portals provide opportunities to revitalize the local government sector and also provide enhanced business partnerships (2003). These increased partnerships provide enhanced service opportunities and allow government to work with businesses in a more collaborative fashion.

Municipal agencies have made large strides in enhancing their e-government offerings. Since 2000 municipal agencies have incrementally increased the number of e-government services they provide and also enhanced the degree of interactivity that they offer (Holden, Norris, & Fletcher, 2003). Research from the early 2000's shows that local government agencies have harnessed technological improvement and enhancements that resulted in cost savings (Mary Maureen Brown, 2001). As with most ventures, the benefits must outweigh the costs to make such technological improvement possible.

Several researchers have noted the evolution in municipal government, which is the rapid adoption and enhancement of e-government services. Others have correlated the progress and advances of e-government services to e-business maturity models (Shackleton, Fisher, & Dawson, 2004). While comparing government usage to e-business can be helpful at times, it is important to recognize that differences do exist. In enhancing online services local government entities are more interested in providing content and services as opposed to commerce (Premkumar, Ho, & Chakraborty, 2006). However despite these differences, municipal government has evolved and developed the degree to which online services are provided.

In looking at e-government at the municipal level, several trends are apparent. For example, Wohlers describes the level of sophistication of e-government among local agencies. He argues that the level of sophistication of e-government agencies is positively correlated with agencies that are overseen by professional managers and provided with more organizational resources (Wohlers, 2007). His findings and arguments are logical. Municipal agencies which have more resources in terms of support, staff and budget are those that are most technological sophisticated and provide the most robust e-government offerings. Along those lines, local government agencies with more limited resources and staff were less likely to have e-government services or provided them at a reduced capacity. Additional research performed by Wohlers also continues to suggest this pattern (Wohlers, 2010).

In looking at trends, it is important to recognize that the types of services found at the municipal level are varied. The varied nature of e-government offerings becomes readily apparent when looking at municipal e-government at a global scale. Each municipal agency provides offerings that are most relevant and helpful to their particular citizen base (Mann, Grant, & Mann, 2011). So while there is a common trend in increased offerings and usage of e-government services, the precise offerings can vary greatly from one municipality to another.

Recent studies and publications continue to demonstrate the interest in e-government at the municipal government level. Municipal government agencies are concerned with and aware of the needed to offer online services (Norris & Reddick, 2012). One such reason for the increased desire for e-government is the data mining potential. As citizens increase their usage of e-government the potential to mine important demographic and geographic data increases (Bakırlı et al., 2012). This information provides opportunities for local agencies to better understand their citizen base and understand their needs. E-government has also been cited not only for its data mining capabilities but for its ability to assist agencies in knowledge management activities (Anttiroiko, 2002). Therefore, government mines data from citizens, but at the same time provides access to more information and resources in a digital fashion.

Another reason for why municipal agencies adopt e-government systems is because of the value they offer both to the organization in question and to their citizen base. The value approach to local e-government has been modeled by some and research suggests that taking such an approach ensures that the value that such a system provides is properly captured (Castelnovo & Simonetta, 2007). In most instances e-government when properly implemented brings value to the agency. In some limited instances, when the needs of the community are not properly assessed, some e-government projects can be unsuccessful due to limited utilization by the public. Despite the occasional e-government mishap, many benefits are still seen in the majority of municipal e-government projects (Cook, LaVigne, Pagano, Dawes, & Pardo, 2002).

Municipal agencies still face many barriers and obstacles to implementing their e-government projects. A difficult aspect of this is that there is such a disparity in the capacity, both technological and human from one municipality to another (Kim & Bretschneider, 2004). Such disparities cause it to be difficult to anticipate or foresee potential organizational limitations that may occur during a given e-government implementation. However, projects that occurred at agencies with strategic planning initiatives and executives with IT experience were more likely to overcome barriers and obstacles encountered during implementation of e-government systems (Beaumaster, 2002).

Of the many barriers or challenges cited, privacy and security of e-government systems were a recurring theme (Edmiston, 2003). Municipalities often rely heavily on third-parties to host, maintain and service many aspects of e-government systems. Outsourcing these services while not uncommon, also presents many security concerns. Assessing security of third-party systems can be difficult since most municipal agencies are not even familiar with what type of security they should ask for and end up following any recommendations provided by the vendor.

Security related challenges are not unknown and are frequently highlighted as a problem for municipal or local government agencies (Jain & Kesar, 2008, 2011). As noted earlier, research and publications specific to municipal e-government is scarce. Research specific to security as it relates to municipal e-government is even more limited. The limited nature of publications relating to municipal e-government security and the frequent mention of security as a barrier to e-government initiatives hints at a need for further research in this area. While local government agencies are capable of implementing e-government solutions, many opportunities exist to refine the degree of security in place for such systems.

Research Gaps

As seen throughout this section, an extensive literature review and search was conducted in preparing this study. This section commenced with providing an overview of e-government and defining the term electronic government. A careful consideration of the various models used to describe, classify and interpret e-government systems was also given. Furthermore discussion and research was presented highlighting common barriers that arise when implementing and maintaining e-government systems. Lastly, a look at e-government systems at the municipal government level was considered along with highlights from key literature in the area.

However, this review of literature also identified gaps in the extant publications in the area of e-government. In a general sense, the e-government body of knowledge is composed of over 5,524 publications. Of those publications less than eight percent (8%) focus on municipal government (see Table 2.1). In looking at publications that focus on security, less than 5 percent (5%) of the total publications had a security foucs.

Table 2.2: Security Focused Publications in the EGRL

Keyword	Number of Publications	Percentage of Total EGRL Library*
Privacy	70	1.27%
Security	128	2.32%
Risk	52	0.94%
Threat	10	0.18%
Vulnerability(ies)	4	0.07%
Total	**264**	**4.78%**
		*Total number of literary sources in the EGRL = 5,524

As such, this literature review finds that two key deficiencies or gaps in the extant body of knowledge in e-government are as follows: *security* and *municipal government*. The findings and results of this research effort provide a significant contribution in both of these two gap areas of security and municipal government. Nevertheless, it is necessary for future publications and research efforts to hone in on the importance of security in e-government systems. Additionally, a growth in the body of e-government publications that address local, municipal and city government is also needed.

CHAPTER 3

RESEARCH METHODOLOGY AND DESIGN

Case Study Design

This research project analyzed municipal e-government security using a descriptive case study research approach. The research focused on understanding e-government within a municipal context to ascertain an improved understanding of how e-government is influenced by this context (M. Myers, 1997). Additionally, this study adopted an interpretive research philosophy.

Case study research is an instrumental research model which is frequently used in information systems research (Orlikowski & Baroudi, 1991). This particular study utilized the case study research recommendations set forth by Walsham (1995) for interpretive case study research. Walsham prescribes a series of guidelines for interpretive studies to ensure that the role of the researcher is clearly defined. Following this set of recommendations ensured that generalizations could be formulated from the research findings.

Municipal e-government security will be analyzed as described earlier using a descriptive case study approach. Walsham (1995) supports an interpretive approach when conducting case study research "since it has been widely drawn on by organizational researchers concerned with interpreting the patterns of symbolic action that create and maintain a sense of organization".

In designing this particular case study the recommendations set forth by Yin (2009) were utilized. Yin enumerates five key components of such a design:

1) Research Question(s)
2) Propositions (if any)
3) Unit(s) of Analysis
4) Logically Linking Data to Propositions
5) Criteria for Interpreting Findings

Research Questions. Yin (2009) indicates that case study research is best suited to answer "how" and "why" questions. It is recognized that significant regulation is in place which requires federal agencies to comply with various security standards for their e-government solutions.

The interest of this specific study is to take an in-depth look at e-government security practices for municipal government agencies using these three research questions.

1) What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?
2) How can municipal agencies reach a federal level of e-government security?
3) Why are municipalities not fully compliant with federal e-government security requirements?

It is important to note that the first research question is not one that would typically be addressed by a case study research approach. However, this research question was addressed as part of the study as it was necessary to baseline the current state of the municipalities that will be selected for this study.

Study Propositions. A principle component of this study focuses on the need to shed additional attention to and research on municipal e-government security. Earlier, it was identified that federal agencies have been provided ample regulation and also guidance for implementing security measures for their e-government initiatives. Due to the limited nature of extant research on municipal e-government security this study will take a descriptive approach. However, some propositions and assumptions will still be made.

Proposition 1: The general lack of research interest and attention has caused many municipal government agencies to fall short on their security.

Proposition 2: The gap in federal and municipal e-government security is a result of the lack of guidance and research coupled with limited resources for implementing such security.

Unit of Analysis. Identifying the actual component of what a "case" consists of can sometimes be a challenging task for the researcher. However, defining a unit of analysis is a critical component of a case study research design (Yin, 2009). The point of analysis for this particular study is municipal government agencies. The case that will be analyzed is that of municipalities within the county of Orange of the state of California. This is a large county within southern California which has 34 incorporated cities of various sizes. As such the focal point of analysis will be each individual municipality within this county. Additionally one key stakeholder will be selected from each agency to be interviewed.

Logically Linking Data to Propositions. Two propositions were described earlier. The first proposes a general lack of interest in security for e-government agencies. The second purports that one of the reasons for which municipal government agencies struggle with security is because of their limited organizational resources and lack of security guidance. The study encompasses the 34 incorporated municipalities within Orange County, California. The E-Government Security Act of 2002 requires federal agencies to provide security protocols to protect information. This requirement can be met by adhering to the guidelines of NIST Special Publication 800-44, Guidelines on Securing Public Web Servers. This publication provides a series of seven (7) security checklists which a federal agency must follow to comply with the E-Government Security Act of 2002, 207(f)(1)(b)(iv).

As such, a comparative analysis of each organization to the NIST Publication 800-44 security checklists was performed to: 1) baseline each municipality and 2) identify how agencies in general can become more compliant.

Criteria for Interpreting Findings. The findings of this case study will be closely correlated to each agency's compliance or lack thereof to the NIST 800-44 standard. Here an opportunity will be afforded to assess whether municipal government agencies can in fact comply with the federally required NIST 800-44 standard. It will also ensure that each organization is equally analyzed against a set of common criteria. The NIST 800-44 publication provides a series of seven (7) security checklists which can be used by an organization to gauge compliance with this standard. The degree of deviation or compliance with these security checklists will serve as the key basis for interpreting the findings of this study.

To provide a complete overview and picture of each of the 34 municipalities, this summary is provided to indicate the information that has been gathered from each agency. The case study will therefore include relevant information from each city such as follows:

Quantitative Data Collection

The collection of data and information for this research project was divided into two sections. The first step was to establish contact with each municipality within Orange County. After an appropriate contact person was located, they were provided with a pre-interview participant survey. This survey collected some precursor information prior to the interview. Below a listing of the information that was collected from the pre-interview participant survey.

- Point of Contact Information
  - First Name
  - Last Name
  - Job Title
  - Phone Number
  - Email Address
- Name of Municipality
- Staffing Resources
  - Number of IT staff or contractors
  - Dedicated Information Security Officers (if any)
- Financial Resources
  - Total City Budget
  - Total IT Budget
- Ease of Implementation for NIST SP800-44 Security Checklist Items
  - Checklist 1 - Planning and Managing Web Servers
  - Checklist 2 - Securing the Web Server Operating System
  - Checklist 3 - Securing the Web Server
  - Checklist 4 - Securing Web Content
  - Checklist 5 - Using Authentication and Encryption Technologies for Web Servers
  - Checklist 6 - Implementing a Secure Network Infrastructure

- Checklist 7 - Administering the Web Server

The NIST Special Publication 800-44 is utilized by federal government agencies to comply with the security requirements set forth by the E-Government Security Act of 2002. Municipal agencies are not required to comply with these security requirements. However, these security requirements were used as the baseline for "secure" e-government systems. The NIST SP 800-44 contains a series of seven (7) security checklists. Each checklist contains major security areas with smaller objectives or tasks that should be performed at each level. The pre-interview participant survey asked each stakeholder to rate the degree of difficulty to complete each major sub-category for each of the seven security checklists.

Table 3.1 shown below provides the name of each of the security checklists. Additionally, it also provides the major checklist categories. The participants were asked to rate the degree of difficulty to complete each of these major checklist items in the pre-interview participant survey.

Table 3.1 – NIST SP800-44 Major Checklist Categories

Checklist 1 - Planning and Managing Web Servers
Plan the configuration and deployment of the Web server
Choose appropriate OS for Web server
Choose appropriate platform for Web server
Checklist 2 - Securing the Web Server Operating System
Patch and upgrade OS
Remove or disable unnecessary services and applications
Configure OS user authentication
Configure resource controls appropriately
Install and configure additional security controls
Test the security of the OS
Checklist 3 - Securing the Web Server
Securely install the Web server
Configure OS and Web server access controls
Configure a secure Web content directory
Checklist 4 - Securing Web Content
Ensure that none of the following types of information are available on or through a public Web server
Establish an organizational-wide documented formal policy and process for approving public Web content that—(see items below)
Maintain Web user privacy
Mitigate indirect attacks on content

Client-side active content security considerations
Maintain server-side active content security
Checklist 5 - Using Authentication and Encryption Technologies for Web Servers
Configure Web authentication and encryption technologies
Configure SSL/TLS
Protect against brute force attacks
Checklist 6 - Implementing a Secure Network Infrastructure
Identify network location
Assess firewall configuration
Evaluate intrusion detection and prevention systems
Assess network switches
Evaluate load balancers
Evaluate reverse proxies
Checklist 7 - Administering the Web Server
Perform logging
Perform Web server backups
Recover from a compromise
Test security
Conduct remote administration and content updates

Qualitative Information Collection

The second portion of the data collection involved following up with each individual that completed the pre-interview participant survey. To obtain a qualitative understanding of the nature of a given municipality an attempt was made to speak to the key stake holder responsible for the oversight of information technology (IT) related operations. In most municipalities this typically consisted of an IT manager, IT director, IT administrator, or IT analyst. In instances, where a municipality utilized solely contract IT staff, the administrator or responsible party within the organization for managing that contact was contacted. In instances, where neither of these individuals was available, the desired information was obtained from the public relations/information office.

Participant Interview Questions

1) What do you feel is the greatest challenge in implementing and maintaining e-government security for your agency?

2) What organizational change or resource would assist your agency in enhancing its e-government security?

Prior to commencing the interview, the participant was given a brief overview of e-government and the purpose of the study. The participants were also ensured that anonymity would be maintained and that no one agency would singled-out and that the study was not intended to cause harm or report negligent behavior.

CHAPTER 4

RESULTS, ANALYSIS AND FINDINGS

The results of this study are substantial and enhance the e-government research community in two key facets: results contributing to practice and results contributing to research and theory.

Results Contributing to Practice

In gathering data and information to answer the three (3) research questions proposed by this study, a significant amount of data was captured regarding the utilization of e-government and key demographics of each of the 34 incorporated cities of Orange County, California. All 34 cities utilized e-government services to some degree. Each organization had at minimum a public facing city website which provided at least read-only information to their citizen base. Many other agencies utilized e-government services which facilitated financial transactions and two-way communication.

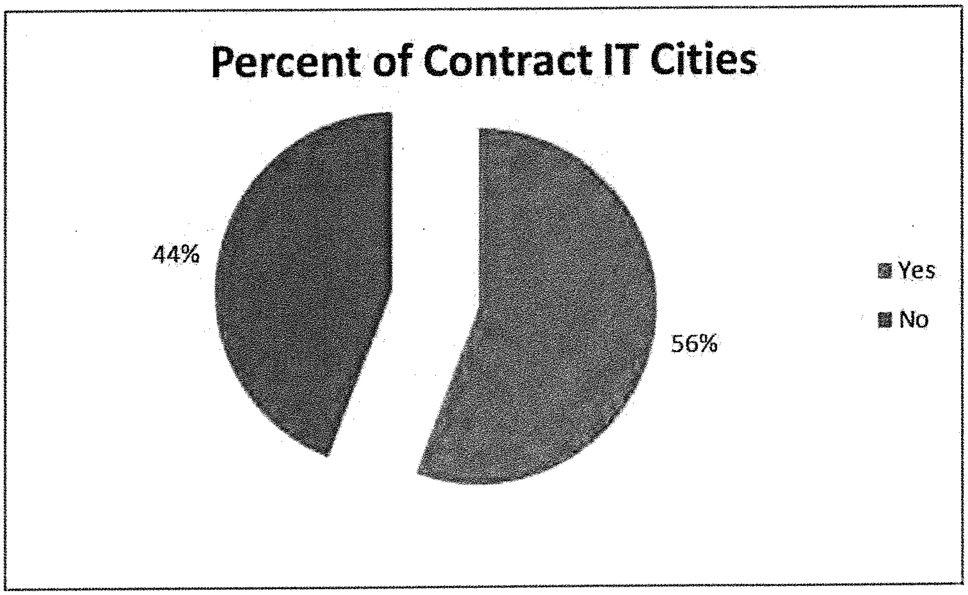
Table 4.1 shown below provides an overview of the 34 cities that were covered as part of this case study. The table furnishes information regarding each city's population based from 2010 United States Census data. Additionally, budgetary information for the entire city and the IT division were provided where available. Cities with larger populations had correspondingly larger organizational budgets and also larger budgets for IT expenditures. The budget for IT expenditures is useful because e-government services, maintenance and security are typically funded through the city's IT budget. Those with larger IT budgets were seen to have a larger IT staff and more robust IT and e-government systems in place.

Table 4.1 – City Demographics and Budgetary Information

City Name	Population (U.S. Census 2010)	Website	E-Government Services	Budget Fiscal Year 2011-12	IT Budget Fiscal Year 2011-12
Aliso Viejo	47,823	Yes	Yes	$ 13,440,955	$ 833,339
Anaheim	336,265	Yes	Yes	$ 1,305,839,186	$ 14,614,442
Brea	39,282	Yes	Yes	$ 84,671,801	unavailable
Buena Park	80,530	Yes	Yes	$ 121,963,350	$ 1,124,700
Costa Mesa	109,960	Yes	Yes	$ 94,650,182	$ 4,881,835
Cypress	47,802	Yes	Yes	$ 33,129,770	$ 560,000
Dana Point	33,351	Yes	Yes	$ 27,367,550	$ 225,000
Fountain Valley	55,313	Yes	Yes	$ 33,863,160	$ 956,657
Fullerton	135,161	Yes	Yes	$ 193,200,000	unavailable
Garden Grove	170,883	Yes	Yes	$ 88,950,000	$ 2,373,663
Huntington Beach	189,992	Yes	Yes	$ 183,547,977	$ 5,867,138
Irvine	212,375	Yes	Yes	$ 136,206,801	$ 11,630,000
La Habra	62,979	Yes	Yes	$ 33,564,360	$ 1,200,000
La Palma	77,264	Yes	Yes	$ 13,432,204	$ 253,300
Laguna Beach	60,239	Yes	Yes	$ 64,322,200	$ 170,300
Laguna Hills	15,568	Yes	Yes	$ 35,650,191	$ 271,000
Laguna Niguel	22,723	Yes	Yes	$ 41,043,398	$ 320,000
Laguna Woods	30,344	Yes	Yes	$ 7,569,992	$ 24,000
Lake Forest	16,192	Yes	Yes	$ 33,798,900	$ 945,000
Los Alamitos	11,449	Yes	Yes	$ 15,629,823	$ 173,000
Mission Viejo	93,305	Yes	Yes	$ 90,150,514	$ 3,400,000
Newport Beach	85,186	Yes	Yes	$ 148,955,783	$ 5,000,000
Orange	136,416	Yes	Yes	$ 170,949,929	$ 2,000,000
Placentia	50,533	Yes	Yes	$ 57,654,595	unavailable
Rancho Santa Margarita	47,853	Yes	Yes	$ 17,206,488	$ 170,215
San Clemente	63,522	Yes	Yes	$ 114,343,420	$ 999,000
San Juan Capistrano	34,593	Yes	Yes	$ 58,757,473	$ 1,000,000
Santa Ana	324,528	Yes	Yes	$ 459,361,890	unavailable
Seal Beach	24,168	Yes	Yes	$ 60,662,300	$ 125,000
Stanton	38,186	Yes	Yes	$ 22,446,727	$ 101,500
Tustin	75,540	Yes	Yes	$ 143,631,002	$ 1,300,000
Villa Park	5,812	Yes	Yes	$ 3,934,000	$ 30,000
Westminster	89,701	Yes	No	$ 127,712,077	unavailable
Yorba Linda	64,234	Yes	Yes	$ 110,581,212	$ 60,000

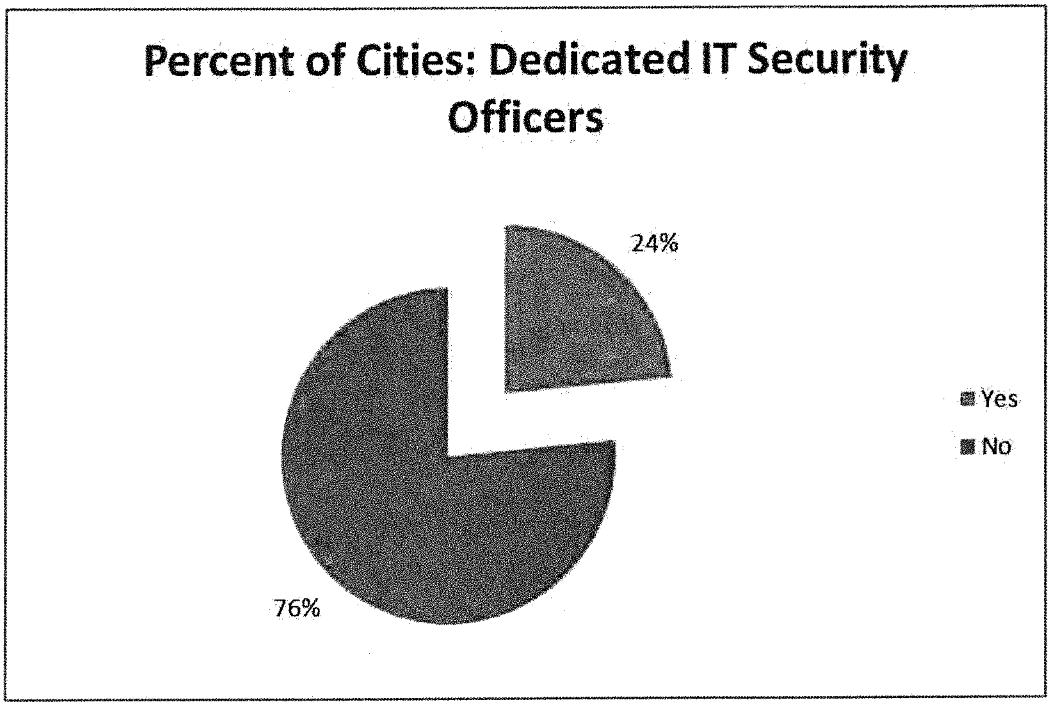
It is also interesting to note the number of cities contracting out all IT services. Of the 34 Orange County cities, 19 of them contracted out all IT services and 15 utilized in-house staff to provide IT support. The figure 4.1 depicted below provides a visual break-down of the distribution of contract and non-contract IT cities.

Figure 4.1 – Percent of Cities Using All Contract IT Services



In investigating the capacity to provide e-government security for their agency, participants of the case study were asked during the pre-interview participant survey to indicate whether or not their organization had a dedicated IT security officer. Of the total 34 incorporated cities, only eight (8) agencies had dedicated IT security officers and 26 of them indicated that they did not have a dedicated IT security officer. For the purposes of this study, an IT security officer was defined as a staff member whose primary responsibility was to maintain and provide IT security for their agency. Figure 4.2 shown below provides an overview of the distribution between those cities that have dedicated IT security officers and those that do not.

Figure 4.2 – Percent of Cities with Dedicated IT Security Officers



Additional information regarding the staffing resources within each organization as it pertains to IT support was also gathered through the pre-interview participant survey. The city with the highest number of IT employees/staff had a total of 64 staff members. The city with the least amount of IT support had the full-time equivalent (FTE) of 0.4 IT staff members. The average number of IT staff members was 9.68 with a standard deviation among agencies of 13.11. Table 4.2 provides an overview of the descriptive statistics for the IT staffing resources for the 34 incorporated municipalities within Orange County. In collecting these figures, no distinction was made between contract and non-contract IT staff.

Table 4.2 – Descriptive Statistics for City IT Staffing Resources

Descriptive Statistics for IT Staffing	
Average	9.68
Range	0.4 to 64
Min	0.4
Max	64
Standard Deviation	13.1141946

The results of this study contributing to practice provide an overview of the financial, demographics and staffing resources available to promote and maintain e-government security by each of 34 the agencies that were included in the study. Additionally, insight was also provided into the size of each agency and whether or not a dedicated IT security officer was held by the agency. The varying degree of resources and size show that even when looking at the smallest level of government: municipal government, a great degree of variation exists from agency to agency. Cities that were larger both in citizen base and geographical size had larger organizational budgets and more IT staff. Smaller cities were more financially restricted and had more limited IT staff and resources.

Results Contributing to Research and Theory

The primary output of this research project was the development of a theoretical model which addressed the three (3) key questions surrounding municipal e-government security that were presented during the onset of this study.

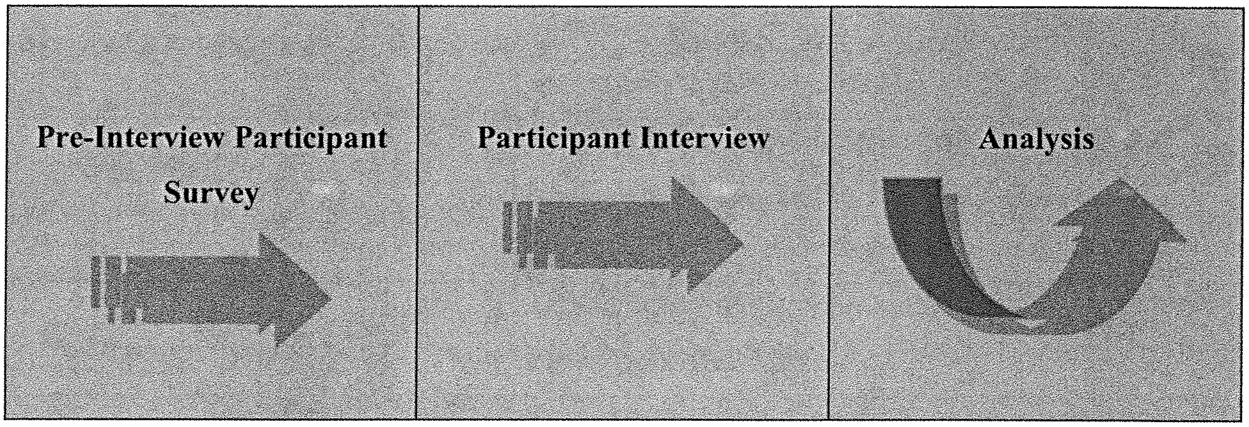
The three (3) research questions that were investigated by means of this case study were:

1) What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?
2) How can municipal agencies reach a federal level of e-government security?
3) Why are municipalities not fully compliant with federal e-government security requirements?

These three questions addressed the "what", "how" and "why" of municipal e-government compliance as it related to the seven (7) security checklists of the NIST 800-44 publication.

Figure 4.3 illustrates the progression of the research initiative. Prior to interviewing each of the participants, each participant was asked to complete a pre-interview survey. Upon completion and receipt of the survey an interview was conducted with the participant.

Figure 4.3 – Research Process Flow



The findings and results of this section will be divided into two sub-sections: Results and Findings from the Pre-Interview Participant Survey and Results and Findings from the Participant Interviews.

Results and Findings: Pre-Interview Participant Survey

Each case study participant was asked to respond to a standardized set of questions to allow the research to: 1) understand the general composition of the organization and 2) to assess the degree of difficulty in complying with the various major sub-sections of the seven (7) security checklists from the NIST SP800-44 publication. Appendix A of this study provides a copy of the Pre-Interview Participant Survey that was distributed to each case study participant. In appendix B of this study a copy of the seven (7) security checklist as found in the NIST SP800-44 publication are provided. Appendix C of this study provided a aggregated list of the security checklist items and identify the major sub-categories within each checklist.

In total, participants were asked to provide the degree of ease or difficulty related to 32 security category items. Each security category item corresponds to a major sub-section of a given security checklist from the NIST SP800-44 publication. Participants were allowed to select from one of four options: completed, easy, medium and difficult. Definitions are provided below in Table 4.3.

Table 4.3 – Definition of Survey Response Options

Survey Response Option	Definition
Completed	This response option indicates that the agency is compliant and has implemented the item requested by the security checklist in this area.
Easy	This response option indicates the agency has not implemented or taken this security measure as indicated in the security checklist. However, the agency believes that implementing this requirement can be done relatively easily.
Medium	This response option indicates the agency has not implemented or taken this security measure as indicated in the security checklist. However, the agency believes that implementing this requirement can be completed with a medium or average level of difficulty.
Difficult	This response option indicates the agency has not implemented or taken this security measure as indicated in the security checklist. However, the agency believes that implementing this requirement would be difficult considering present budgetary, technological and staffing resources.

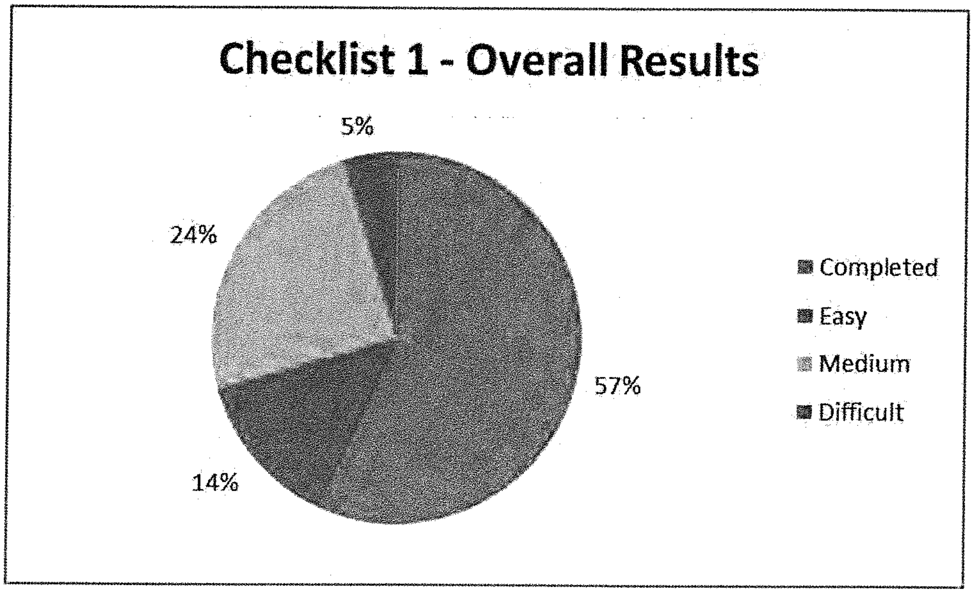
A high-level overview of the results from the pre-interview participant survey is shown below on Table 4.4. Of all the 34 agencies included in the study, none of them were compliant in all areas. The table shows the percentage of scores for each rating distributed among each of the 32 major sub-sections from the seven (7) security checklists of the NIST SP800-44 publication.

Table 4.4 – Overview of Pre-Interview Participant Survey Results

Checklist 1 - Planning and Managing Web Servers	**Completed**	**Easy**	**Medium**	**Difficult**
Plan the configuration and deployment of the Web server	64.71%	2.94%	29.41%	2.94%
Choose appropriate OS for Web server	61.76%	17.65%	17.65%	2.94%
Choose appropriate platform for Web server	44.12%	20.59%	26.47%	8.82%
Checklist 2 - Securing the Web Server Operating System				
Patch and upgrade OS	35.29%	29.41%	11.76%	23.53%
Remove or disable unnecessary services and applications	38.24%	50.00%	11.76%	0.00%
Configure OS user authentication	41.18%	52.94%	5.88%	0.00%
Configure resource controls appropriately	35.29%	55.88%	8.82%	0.00%
Install and configure additional security controls	73.53%	23.53%	2.94%	0.00%
Test the security of the OS	32.35%	23.53%	29.41%	14.71%
Checklist 3 - Securing the Web Server				
Securely install the Web server	32.35%	14.71%	20.59%	32.35%
Configure OS and Web server access controls	20.59%	23.53%	17.65%	38.24%
Configure a secure Web content directory	29.41%	23.53%	14.71%	32.35%
Checklist 4 - Securing Web Content				
Ensure that none of the following types of information are available on or through a public Web server	38.24%	8.82%	20.59%	38.24%
Establish an organizational-wide documented formal policy and process for approving public Web content	20.59%	11.76%	55.88%	11.76%
Maintain Web user privacy	23.53%	29.41%	38.24%	8.82%
Mitigate indirect attacks on content	17.65%	11.76%	41.18%	29.41%
Client-side active content security considerations	29.41%	20.59%	20.59%	29.41%
Maintain server-side active content security	26.47%	5.88%	29.41%	38.24%
Checklist 5 - Using Authentication and Encryption Technologies for Web Servers				
Configure Web authentication and encryption technologies	35.29%	17.65%	8.82%	38.24%
Configure SSL/TLS	32.35%	14.71%	17.65%	35.29%
Protect against brute force attacks	23.53%	26.47%	38.24%	11.76%
Checklist 6 - Implementing a Secure Network Infrastructure				
Identify network location	91.18%	0.00%	5.88%	2.94%
Assess firewall configuration	79.41%	11.76%	5.88%	2.94%
Evaluate intrusion detection and prevention systems	26.47%	14.71%	17.65%	41.18%
Assess network switches	38.24%	17.65%	5.88%	38.24%
Evaluate load balancers	20.59%	8.82%	41.18%	29.41%
Evaluate reverse proxies	23.53%	23.53%	35.29%	17.65%
Checklist 7 - Administering the Web Server				
Perform logging	26.47%	14.71%	44.12%	14.71%
Perform Web server backups	50.00%	35.29%	11.76%	2.94%
Recover from a compromise	20.59%	14.71%	17.65%	47.06%
Test security	29.41%	17.65%	38.24%	14.71%
Conduct remote administration and content updates	55.88%	17.65%	20.59%	5.88%

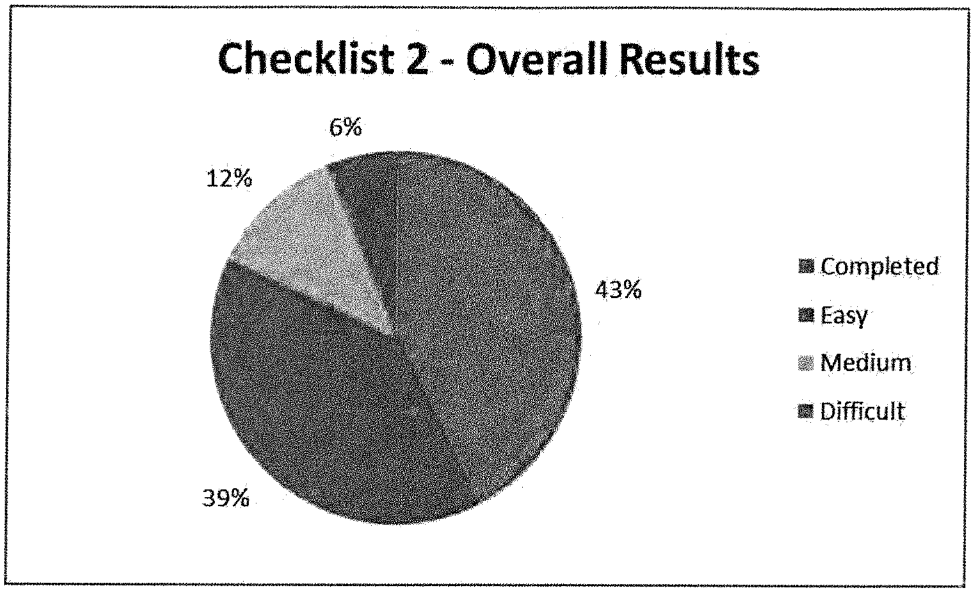
Checklist 1 focused on agencies providing planning and management of web servers. Figure 4.4 shows the overall distribution of results for this survey. Results were aggregated for each of the major sub-categories to provide an overall representation for the entire checklist. In Checklist 1, 57 percent of the responses indicated that agencies had already completed all items of this security checklist. Of the total results for Checklist 1, only 5% in total indicated that it would be difficult to implement all the requirements of this checklist.

Figure 4.4 – Aggregate Survey Results: NIST SP800-44 Checklist 1



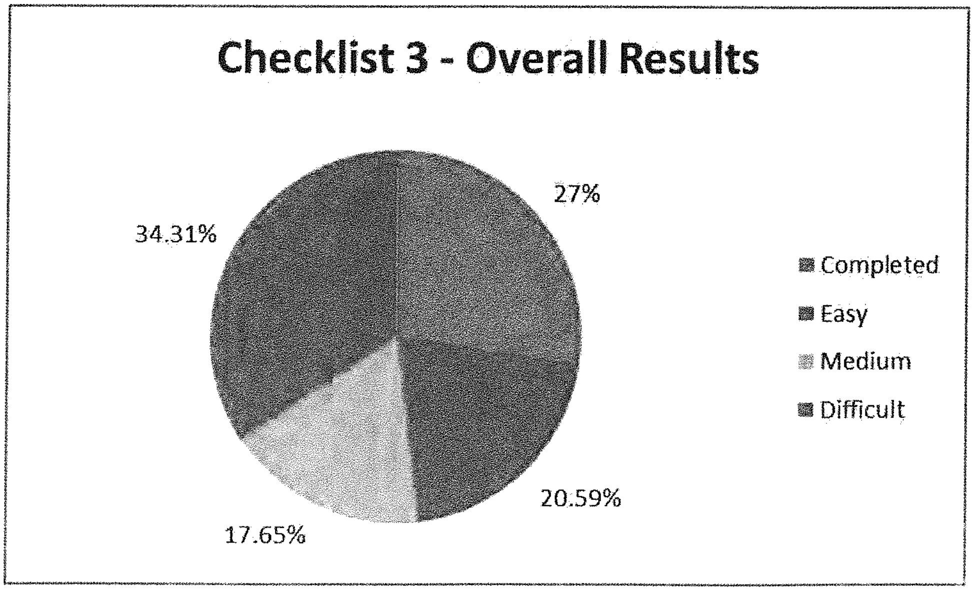
In Checklist 2 the primary focus was securing the web server operating system. This included patching and upgrading the operating system and a test of operating system security. For this checklist a total of 43 percent of all responses indicated compliance with the security requirements. Additionally, 39 percent of the responses indicated that it would be "easy" to become compliant with all requirements of Checklist 2.

Figure 4.5 – Aggregate Survey Results: NIST SP800-44 Checklist 2



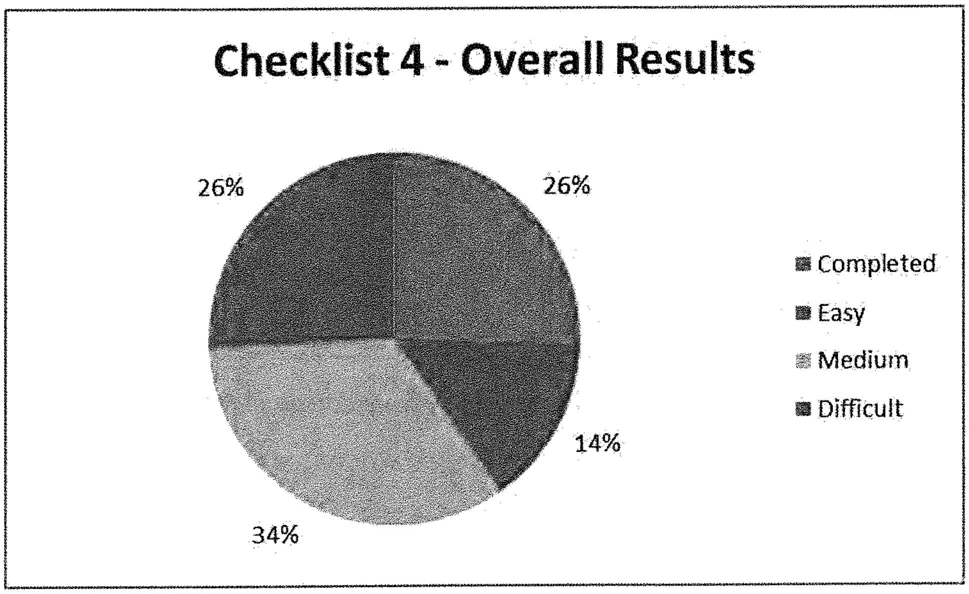
Checklist 3 looked at the measures for securing the web server. This included securely installing the web server, configuring the appropriate access controls and securing the content directory. For this checklist, 27 percent of the response indicated compliance while 34.31 percent of the responses indicated that it would be difficult to become compliant.

Figure 4.6 – Aggregate Survey Results: NIST SP800-44 Checklist 3



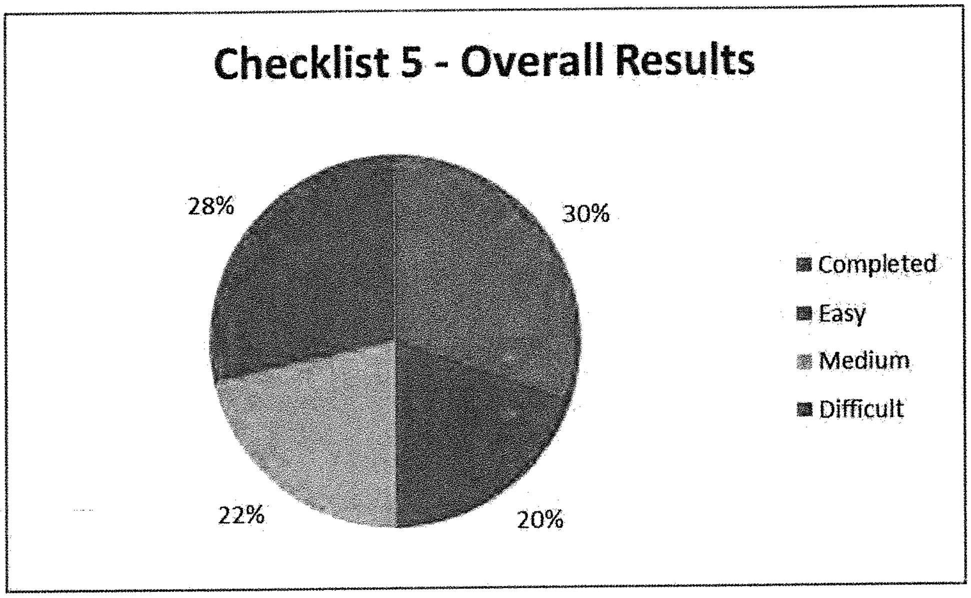
In contrast to the other checklists, Checklist 4 focused on the security of the web content. Some of the sub-items included ensuring proper privacy of web server documents, maintaining web user privacy and the consideration of client-side security. For this checklist, 26 percent of the responses demonstrated compliance in this area. However an equal amount (26 percent) indicated that it would be difficult to reach compliance in this area.

Figure 4.7 – Aggregate Survey Results: NIST SP800-44 Checklist 4



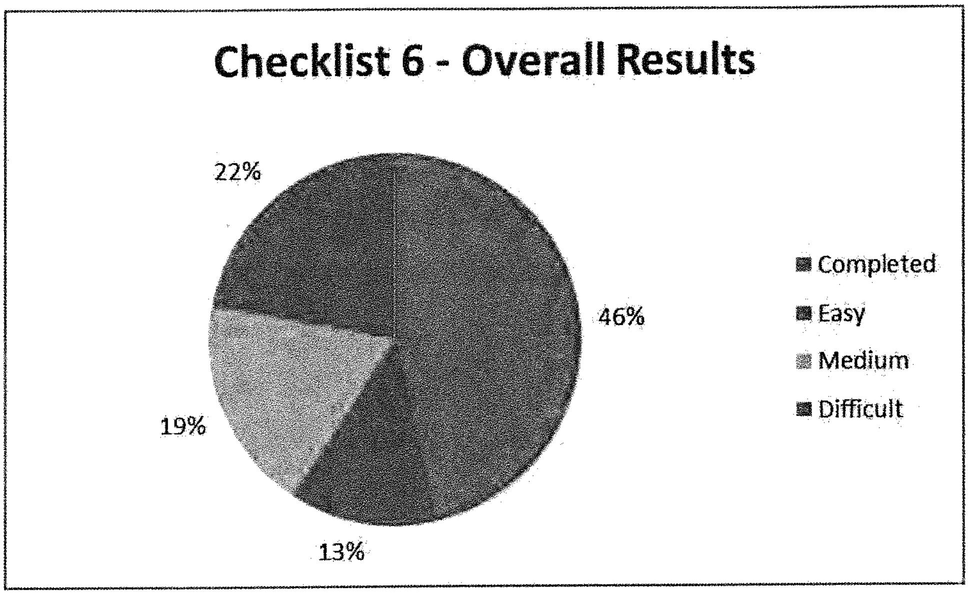
For Checklist 5 the key goals were to ensure proper user authentication and encryption. This included providing mechanisms to authenticate users, encrypt communications and guard against brute force attacks. For this checklist 30 percent of the responses overall indicated compliance while 28 percent of the responses showed that it would be difficult to achieve compliance in this area.

Figure 4.8 – Aggregate Survey Results: NIST SP800-44 Checklist 5



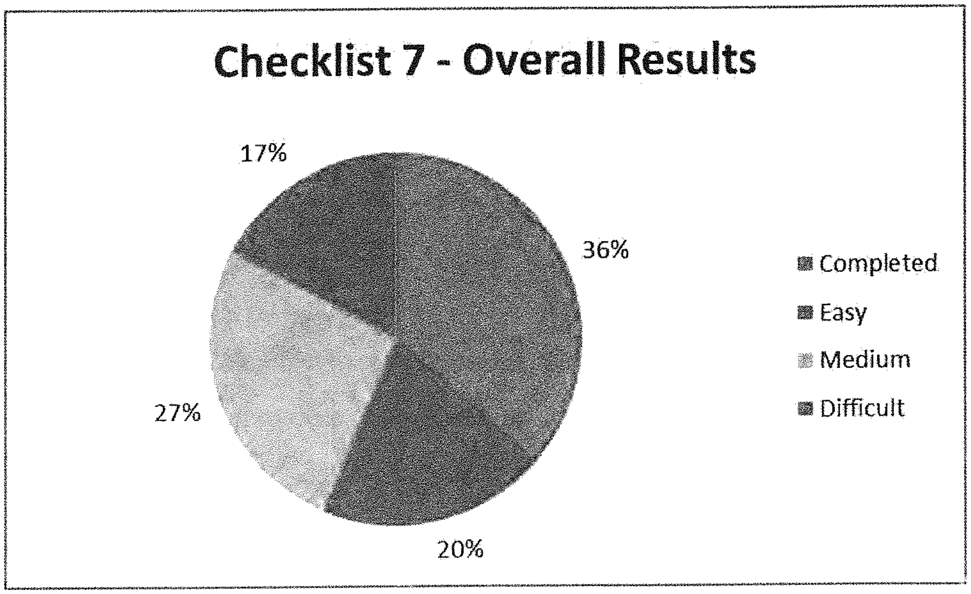
In Checklist 6 agencies were asked to look at the security of their network infrastructure of which their web servers and e-government services were connected to. Some key aspects of this list were to provide a secure location for the network, provide an assessment of the firewall configuration, evaluate of intrusion detection/prevention systems and review reverse proxies. Here 46 percent of the responses showed compliance with 22 percent responding that it would be difficult to comply in this given area.

Figure 4.9 – Aggregate Survey Results: NIST SP800-44 Checklist 6



The final checklist, Checklist 7 focused on the administration of the web server. Evaluation and compliance was sought in areas of logging, web server backups, security testing and remote administration and content updates. Of the responses, 36 percent indicated compliance with 17 percent indicating that it would be difficult to comply with this checklist and its requirements.

Figure 4.10 – Aggregate Survey Results: NIST SP800-44 Checklist 7



The pre-interview participant survey provided significant insight into the degree of compliance with the seven (7) security checklists and the degree of difficulty to become compliant in the various areas. It is important to note that a response of: easy, medium or difficult in any checklist subarea indicates non-compliance in that area. Checklists 1, 2 and 6 showed the greatest degrees of compliance. Compliance overall for these three checklists were 57 percent, 43 percent and 36 percent respectively. The greatest degree of difficulty in achieving compliance was noted in Checklists 3, 4 and 5. The percentage of responses indicating difficulty in achieving compliance in these areas was 34 percent, 28 percent and 22 percent respectively. As evidenced by the survey responses municipal agencies have a large percentage of area within the seven (7) security checklists that were not in compliance. While varying degrees of difficulty in compliance exists, it should be noted that federal government agencies are statutorily required to be 100 percent compliance in all checklists areas.

Rank Analysis

One of the goals of the pre-interview participant survey was to gauge the level of compliance or difficulty in complying with the various areas of the NIST SP800-44 security checklists. The results and charts shown in the previous section provide exploratory information into the degree of compliance amongst the surveyed agencies. However, the survey also gathered information in three key areas which help theorize and understand why agencies have difficulty complying in certain areas. All agencies were asked to provide these three (3) additional key elements:

1) IT Budget
2) Number of IT Employees/Staff
3) Dedicated IT Security Officer

The first rank analysis was performed by ranking all agencies by those having the greatest degree of compliance. The pre-interview participant survey asked participants to rate their compliance or ability to comply with 32 separate items from the NIST SP800-44 security checklists. The three (3) agencies ranked with the greatest number of responses indicating “completed” also had IT budgets that ranked in the top ten of all surveyed agencies.

Naturally, IT budgets varied from agency to agency based on the size of the city and the population of citizens that it serves. Nonetheless, agencies with larger IT budgets were found to have a higher degree of compliance. This signals the important of IT funding and how it affects an organization's ability to maintain e-government security.

Furthermore, staffing is another important consideration when looking at an agency's ability to provide and maintain e-government security. The same agencies that held the top three (3) ranks for compliance also had IT staffing numbers that ranked in the top 10 list. Complying with all aspects of the security checklists requires adequate IT funding and sufficient IT staff to perform the required security procedures. The top three agencies in compliance ranked the highest in both IT funding and IT staffing.

IT budgetary ranking did not appear to affect whether or not an agency had a dedicated information security officer. A total of 8 of the 34 agencies or 24 percent reported having a dedicated information security officer. However, those agencies have information security officers were spread-out through the budgetary rankings.

Additionally, the presence of an IT security officer did not seem to have an impact on an agency's ability to maintain compliance with the security checklists. Table 4.5 shown below provides a ranking of all 34 agencies and indicates whether or not the agency had a dedicated IT security officer. As shown in the table below, even agencies ranking low in compliance had dedicate information security officers. The importance of this finding is not to discount the value that is brought to an organization by having an information security officer. But instead this highlights the fact that even agencies that cannot afford to have a dedicated security officer can still maintain a high-level of e-government security. Therefore, not having a dedicated information security officer in itself does not necessarily prevent an agency from achieving a high-level of compliance.

Table 4.5 – Ranking of Compliance Mapped to Security Officer Presence

Ranking - % of Compliance	Dedicated Security Officer
1	Yes
2	No
2	No
4	No
5	Yes
6	No
7	No
7	No
9	No
10	No
11	Yes
11	No
13	Yes
13	No
15	No
16	Yes
16	No
18	No
19	No
20	No
21	No
22	No
22	No
22	Yes
22	No
22	No
22	No
28	No
28	Yes
28	No
31	No
31	No
33	Yes
33	No

Earlier it was noted that the highest degree of compliance was seen within these security checklists:

- Checklist 1 - Planning and Managing Web Servers
- Checklist 2 - Securing the Web Server Operating System
- Checklist 6 - Implementing a Secure Network Infrastructure

Additionally, the surveyed agencies were seen having the most difficulty in complying with the security checklists shown below:

- Checklist 3 - Securing the Web Server
- Checklist 4 - Securing Web Content
- Checklist 5 - Using Authentication and Encryption Technologies for Web Servers

One goal of this study was to provide an exploratory look at the level of e-government security that municipal agencies currently have in place when compared to federal agencies (*Research Question # 1: What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements*). The pre-participant survey provided ample information and evidence to satisfy research question 1. It also allowed some correlations to be established between the effects that three variables: 1) IT budget, 2) IT staffing and 3) Dedicated IT security officer have on the ability to comply with the NIST security checklist items. However, the results of the participant interviews provided the necessary evidence and information to respond to research questions 2 and 3 in a more thorough manner. Those results are found in the following section.

Results and Findings: Participant Interviews

Following the completion and collection of responses to the pre-interview participant survey, a follow-up was performed to add a qualitative context to the study. Each participant was asked to respond to the following to interview questions:

1) What do you feel is the greatest challenge in implementing and maintaining e-government security for your agency?

2) What organizational change or resource would assist your agency in enhancing its e-government security?

Responses from the participant interviews were coded using the suggestions from (Kumar, 2010). Kumar suggests four steps in coding qualitative data:

1. Identifying the main themes
2. Assign codes to the main themes
3. Classifying responses under the main themes
4. Integrate themes and response into the text of the report

To complete steps 1 and 2 the opening coding method was utilized. Myers prescribes that with open coding the researcher should analyze the responses and summarize the text by the use of a succinct code (M. D. Myers, 2009). In reviewing the responses to the first interview question a total of seven (7) themes were noted. For step 3, Tables 4.7 and 4.9 show a summary of the coding results by participant. To meet the requirements for step 4, the findings from the coded themes have been integrated throughout the narrative of this section.

Table 4.6 summarizes the common themes present among the interviews for interview question 1 along with the code assigned to each theme. This provides a summary of the most prevalent challenges, issues and obstacles that participants discussed during their response to interview question 1.

Table 4.6 – Interview Question 1 – Common Themes and Codes

Interview Question 1 – Common Themes		
Code	Theme	Observations and Findings
Q1T1	1) Staffing	Most agencies (68 percent) commented that limited staffing did not allow for a focus on security.

		Most cities had general IT staff where security was performed as a duty and not a primary role.
Q1T2	2) Budget/Financial	Budgetary and financial challenges were also frequently cited (79 percent). IT funding was generally limited and this became even more limited when looking at funding earmarked specifically for security related initiatives.
Q1T3	3) Training/Expertise	Training and expertise related to security was also listed as a common challenge by 74 percent of the agencies. This percentage of agencies tended to hire IT generalists who do not specialize in security. Thus additional training and staff expertise in IT security was cited as a challenge. As noted earlier in Figure 4.2 only 24 percent of the surveyed agencies had a dedicated information security officer.
Q1T4	4) IT Contract Services	As noted earlier in Figure 4.1, 56 percent of all Orange County cities fully contract out IT services. The 56 percent of cities that contracted out all IT services felt that heavy reliance was placed on the contracting agency to provide security for the agency. However,

		internal staff did not have the expertise to assess the level of security being provided by the contracting agency. Theme Q1T4 was noted by 56 percent of agencies.
Q1T5	5) Vendors	To reduce cost and transfer liability, 59 percent of agencies relied on third-party solutions or hosted services to shift the responsibility to the vendor in case of a security breach. While this approach can be instrumental in some instances, limited agencies had specific service level agreements (SLA) which specifically called out security requirements.
Q1T6	6) Changing Nature of IT Security	While not necessarily specific to e-government security, most agencies commented as the dynamic and changing nature of security as a challenge. New security vulnerabilities and threats are born each day, yet it is hard to stay current with all the latest developments.
Q1T7	7) Time/Resources to Monitor Security Threats	Another commonality was that of time and resources to review security threats and appropriate log files.

Responses varied from municipality to municipality, however several common themes where present that were identified through the coding process. The majority of municipalities realized that staffing and financial limitations were the greatest barrier and challenge in supporting e-government security. This was particularly prevalent in cities that contracted out all IT services. In many instances, the staff members responsible for managing and contracting for such IT services had limited IT knowledge and experience.

Another common challenge that arose was a need for increased training that focused on IT security. Most organizations commented about the ever changing nature of IT security and the heavy reliance on third-party vendors to provide security and support for e-government services. Additionally, a high reliance was placed on the security of the underlining software platforms used to support e-government services. Due to limited resources and time constraints security testing of each e-government service provider was not always possible. Table 4.7 shown below provides an overview of the coding by theme as present in the responses from each of the interviewed participants for question 1.

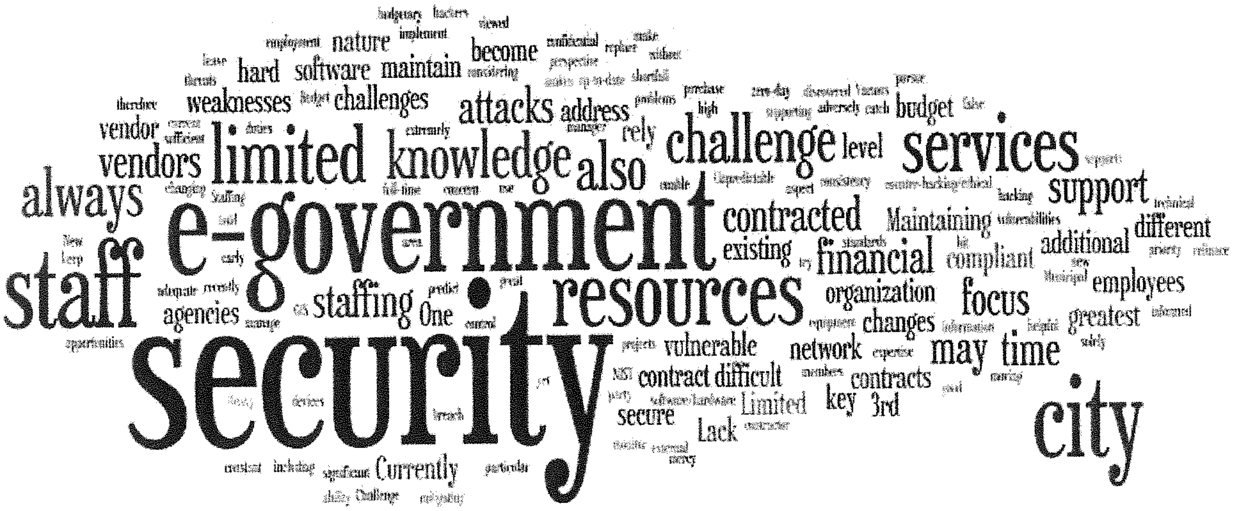
Table 4.7 – Coding Results for Interview Question 1

Participant #	Theme 1 (Q1T1)	Theme 2 (Q1T2)	Theme 3 (Q1T3)	Theme 4 (Q1T4)	Theme 5 (Q1T5)	Theme 6 (Q1T6)	Theme 7 (Q1T7)	Totals
1	1	1	1	1	1	0	1	6
2	0	0	0	0	0	1	1	2
3	0	0	0	0	0	1	1	2
4	1	1	1	1	1	0	1	6
5	1	1	1	0	1	0	0	4
6	1	1	1	1	0	0	1	5
7	0	1	1	0	0	0	0	2
8	1	1	1	0	1	0	1	5
9	0	1	1	0	0	1	1	4
10	0	0	0	0	0	1	1	2
11	1	0	0	0	1	1	0	3
12	1	1	1	1	1	0	1	6
13	0	1	0	0	1	1	0	3
14	1	1	1	1	1	0	1	6
15	1	1	1	1	1	0	1	6
16	1	1	1	1	1	0	1	6

17	1	1	1	1	1	0	1	6
18	1	1	1	1	0	0	1	5
19	1	1	1	1	1	0	1	6
20	1	1	1	1	0	0	1	5
21	1	0	0	0	0	1	0	2
22	0	0	0	0	0	1	0	1
23	1	1	1	1	1	0	1	6
24	1	1	1	1	1	0	1	6
25	1	1	1	1	1	0	1	6
26	0	1	1	0	1	0	0	3
27	1	1	1	1	1	0	1	6
28	0	1	0	0	0	1	0	2
29	1	1	1	1	1	0	1	6
30	1	1	1	1	1	0	1	6
31	0	1	1	0	0	1	0	3
32	1	1	1	1	1	0	1	6
33	1	0	1	1	0	1	1	5
34	0	1	0	0	0	1	1	3
Total	23	27	25	19	20	12	25	

In figure 4.11 a graphical representation of the common words that occurred from the notes of interview question 1 are shown. The use of the website www.wordle.net was selected to highlight key words that were most common throughout interview question 1.

Figure 4.11 – Interview Question 1: Visual Representation of Common Words



Similarities were found between the themes found through the coding process of interview questions 1 and 2. The primary difference is that where question 1 sought input regarding the challenges in maintaining e-government security, question 2 focused on resource(s) that could help improve such security. In interview question 2 there were three (3) common themes: budgeting, staffing and IT security training. Table 4.8 shown below provides an overview of the common themes. It is important to note that correlation between interview questions 1 and 2. The top three resources solicited by cities align well with the top three challenges from interview question 1.

Table 4.8 – Interview Question 2 – Common Themes

	Interview Question 2 – Common Themes	
Code	Theme	Observations and Findings
Q2T1	1) Budgeting	Additional budget and financial support to provide secure e-government services was a top resource which would aid cities in providing enhanced e-government security. Theme Q2T1 was present in 79 percent of the responses to question 2.
Q2T2	2) Staffing	Staffing or additional employees to support e-government security initiatives were also common resources that were listed as being instrumental in enhancing security. Staffing was a primary concern for agencies using fully contract IT staff. Theme Q2T2 was present in 68 percent of the interview responses to question 2.
Q2T3	3) IT Security Training	The majority of respondents

		indicated that they had limited security expertise. In full contract IT cities this was truly an issue as the staff responsible for administering such contracts had limited IT experience. In cities with on-staff IT employees, additional staff training in the area of security was seen as necessary to be able to provide improved e-government security. Theme Q2T3 was noted to be present in 74 percent of the interview responses to question 2.

Table 4.9 which is shown below provides an overview the coding performed for interview question 2. To provide anonymity of each participant, names were not included, but instead these were replaced with random participant numbers.

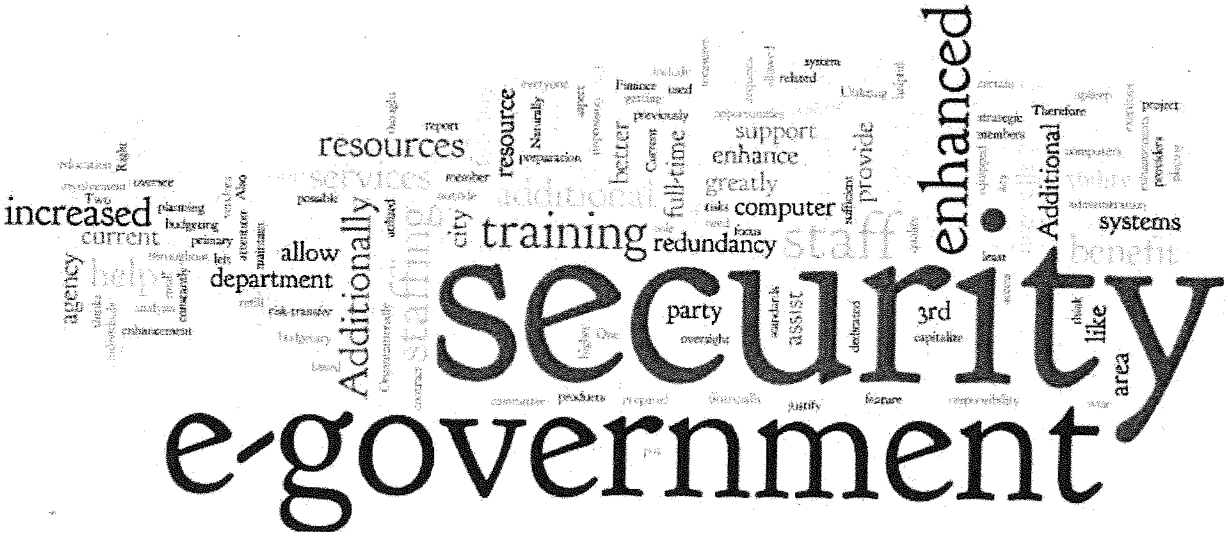
Table 4.9 – Coding Results for Interview Question 2

Participant #	Theme 1 (Q1T1)	Theme 2 (Q1T2)	Theme 3 (Q1T3)	Totals
1	1	1	1	3
2	0	0	0	0
3	0	0	0	0
4	1	1	1	3
5	1	1	1	3
6	1	1	1	3
7	1	0	1	2
8	1	1	1	3
9	1	0	1	2
10	0	0	0	0
11	0	1	0	1
12	1	1	1	3
13	1	0	0	1
14	1	1	1	3
15	1	1	1	3
16	1	1	1	3
17	1	1	1	3
18	1	1	1	3
19	1	1	1	3
20	1	1	1	3
21	0	1	0	1
22	0	0	0	0
23	1	1	1	3
24	1	1	1	3
25	1	1	1	3
26	1	0	1	2
27	1	1	1	3
28	1	0	0	1
29	1	1	1	3
30	1	1	1	3
31	1	0	1	2

32	1	1	1	3
33	0	1	1	2
34	1	0	0	1
Total	27	23	25	

Figure 4.12 shown below provides a graphical representation of the interview notes collected for interview question 2. The larger words from the Wordle signify those that were most common.

Figure 4.12 – Interview Question 2: Visual Representation of Common Words



Summary

This study posed three (3) research questions that were investigated utilizing a descriptive case-study approach. The case study utilized a pre-interview survey and two interview questions to respond to the research questions.

1) What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?
2) How can municipal agencies reach a federal level of e-government security?
3) Why are municipalities not fully compliant with federal e-government security requirements?

To respond to research question 1, participants of the 34 incorporated cities completed a pre-interview survey. This survey provided a current benchmark of e-government security using the NIST SP 800-44 security checklists. Table 4.10 provides an overview of the theoretical model utilized to respond and investigate the three research questions of this study. Key findings show that municipalities did have certain e-government security measures in place. But when compared via the pre-interview survey to federal e-government security requirements large gaps were found.

Additionally, the two interview questions yielded additional insight as to the "how" and "why" of municipal e-government security. Most agencies were aware and desired to have improved security of their e-government systems. However, limited resources and staff time made such efforts difficult. As such these findings provide areas in which municipal government agencies can improve and the resources needed to enhance e-government security.

Table 4.10 – Theoretical Research Model: Aligning Research Questions to Results

Alignment of Research Question to Results and Findings		
Research Question	**Evidence**	**Findings/Results**
Research Question 1: What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?	Pre-interview participant survey.	A significant gap between federal e-government security requirements and municipal compliance was identified. In areas where compliance was not held, agencies listed the degree of difficult associated with achieving compliance. The pre-interview participant survey showed various results that demonstrated compliance gaps as follows: 1) Average completion of all items: 38.05% 2) Average to become compliant rated as "easy": 20.59% 3) Average to become compliant rated as "medium": 20.77% 4) Average to become compliant rated as "difficult": 18.57%
Research Question 2: How can municipal agencies reach a federal level of e-government security?	Interview question 2: What organizational change or resource would assist your agency in enhancing its e-	Three (3) themes were identified through the coding process of the interview responses for research

	government security?	question 2. The resources described as being necessary to achieve an enhanced federal level of e-government security: 1) Budgeting 2) Staffing 3) IT Security Training
Research Question 3: Why are municipalities not fully compliant with federal e-government security requirements?	Interview question 1: What do you feel is the greatest challenge in implementing and maintaining e-government security for your agency Pre-Interview Survey: Ease of Implementation Ratings	The reasons for not being able to comply with the various security requirements were identified via seven (7) themes as identified by the coding of the interview responses to research question 1. The degree of difficulty was also identified via the pre-interview survey. 8) Staffing 9) Budget/Financial 10) Training/Expertise 11) IT Contract Services 12) Vendors 13) Changing Nature of IT Security 14) Time/Resources to Monitor Security Threats

CHAPTER 5

CONTRIBUTIONS, DISCUSSION AND CONCLUSION

Summary of Research Finings

The key purpose of this chapter is to furnish a summary of the research findings as they relate to the three (3) research questions that this study sought to respond to. It also provides the implications of such research findings and makes recommendations based upon findings and implications of this study.

Research Question 1

What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?

This research question was addressed primarily using the pre-interview participant survey. This survey asked the case study participants to rate the level of ease or difficulty associated with each of the 32 major sub-categories of the seven (7) security checklists of the NIST SP800-44 publication. Federal agencies are required to comply with all items of the seven security checklists from this NIST publication. The survey provided a means to assess the degree of compliance and benchmark agencies included in the case study against federal security requirements.

The results of the pre-interview participant survey provided insights into the current state of municipal e-government security. A significant degree of gaps were found between what federal requirements are and what actual security measures municipalities within the study had in place. This evidence provided the impetus to move on to research questions 2 and 3. After all, these remaining two research questions dealt with seeking to understand the reasons as to why municipalities were not up to par with federal e-government security requirements.

Research Question 2

How can municipal agencies reach a federal level of e-government security?

To address this research question, the findings and results from interview question 2 were utilized. Interview question 2 asked participants of the case study to provide the resources that would help enhance e-government security to reach a federal level of security as measured by the NIST SP800-44 publication.

The analysis of interview notes yielded three primary themes amongst the majority of participants:

1) Budgeting
2) Staffing
3) IT Security Training

The first of these was budgeting or funding to provide enhanced e-government security. Most agencies dealt with limited funding to support city-wide IT services. Funding for IT security most always drew from the general IT budget. With multiple demands on this budget, allocating large amounts for security was a difficult task for many agencies.

Staffing, whether agency employees or contract staff was the second most common theme seen throughout interview question 2. Only a small percentage of cities included in the case study had dedicated information security officers. The majority of cities relied on general IT staff to provide support and maintenance of e-government systems including its respective security. Cities that relied only on contract IT staff had the most difficult time in obtaining dedicated resources and attention for e-government security.

Research Question 3

Why are municipalities not fully compliant with federal e-government security requirements?

This particular research question was addressed by means of interview question 1 and the analysis from the pre-interview participant survey. Interview question 1 asked participants of the study to state reasons and challenges to providing and maintaining e-government security. This allowed the researcher to understand the pain points felt by municipal agencies in providing a federal level of e-government security. The analysis of the responses to interview question 1 yielded a total of seven (7) themes or reasons as to why agencies were not fully compliant with federal e-government security requirements.

1) Staffing
2) Budget/Financial
3) Training/Expertise
4) IT Contract Services
5) Vendors
6) Changing Nature of IT Security
7) Time/Resources to Monitor Security Threats

Additionally, the analysis from the pre-interview participant survey provided an overview the degree of difficult associated with each of the major sub-categories from each of the security checklists. This provides reasoning as to why compliance is not held in certain areas due to the degree of difficulty associated with compliance.

Limitations

This study investigated municipal e-government security by utilizing a descriptive case study of Orange County, California municipalities. The selected county had a wide range of cities that varied in size, demographics and population. The study found that while agencies did have security measures in place to protect e-government systems many gaps existed when benchmarked to federal e-government security standards.

This study found three (3) common themes as to "how" agencies can become compliant and the resources that they would need to do so. Additionally, evidence was also provided showing "why" full compliance to federal e-government security requirements did not exist. However, while federal e-government security requirements where used as the benchmark it is important to note that municipal agencies at this time are not statutorily required to adhered to the NIST SP800-44 requirements.

Furthermore, this study recognizes that each municipal agency is different and that the findings from this particular county might not correlate exactly to that of another. Many variables are present that affect a municipal government agency from adopting, implementing and of particular interest to this study, securing e-government systems.

Another issue for consideration in this study is one that was described during the onset of the study. This was the potential of biased responses due to fear or negative repercussions. Throughout each stage of the study, participants were ensured that anonymity and privacy would be provided. The results would be presented in an aggregated format as to not jeopardize the job security of any given individual. However, the possibility still exists that some participants may have been overly cautious in responding to both the survey and interview questions resulting in biased responses. The researcher speculates that if this were to occur, participants would be likely compelled to describe their agency's e-government security in a more compliant fashion.

This study was not designed to be an authoritative study of municipal e-government security to be representative of every municipality. Instead it provides an exploratory look at municipal e-government security through a case study of Orange County, California. Researchers building upon these findings should take due care to carefully analyze and understanding the municipalities which they wish to study.

Recommendations for Future Research

The findings and results of this study proved significant and shed a substantial amount of light on the state of municipal e-government security and the methods that can be utilized to improve municipal e-government security. However, areas for future research and investigation exist. Of the many avenues for future research three key areas or directions are recommended:

1) Cross-state municipal government security: This case study analyzed 34 cities within a single county in California. To supplement the findings and research of this study an analysis of several municipalities across various states is suggested. This would furnish a deeper understanding of municipal e-government security as impacted by various state-level variables. Such a study would also provide results that could be more easily generalized across varying municipalities throughout the United States.

2) NIST SP800-44: This NIST publication was used as the benchmark in reviewing municipal e-government security. This instrument was selected as it is a recognized and federally mandated method to use in providing e-government security at the federal level. However, additional research should focus on the degree of applicability of federal e-government security requirements for municipal agencies. Many gaps in compliance were found amongst the studied municipalities. This perhaps could suggest that achieving full compliance by all municipal government agencies might not be feasible. If so, then a new instrument should be investigated and developed which tailors specifically to the small municipal levels of government.

3) Municipal E-Government Security – The literature review that was prepared for this study evidenced the limited amount of scholarly publications that dealt with municipal e-government security. One method to enhance municipal e-government security and further the research community in this area is to provide additional research and publication in topics pertaining to e-government security. Topics such as challenges, barriers and issues surrounding municipal e-government security would all be beneficial to the research community.

Implications and Conclusion

This study proved to be a significant contribution to the e-government body of knowledge specifically those concerned with municipal e-government security. It provided valuable insight into the state of municipal e-government security by means of a descriptive case study of 34 municipal agencies within Orange County, California. It also utilized the NIST SP800-44 security checklists as required for federal government agencies as the instrument when benchmarking municipal e-government security.

Some of the research findings of this study have already been published and presented at various scholarly conferences as listed in Table 5.1 below.

Table 5.1 – Publications in Municipal E-Government Security

Research and Publications			
Papers			
Conference Name	**Conference Dates**	**Type**	**Title**
Decision Sciences Institute 43rd Annual Meeting and Conference	November 17-20, 2012	Paper	Municipal E-Government Security: A Literature Review and Research Agenda
The 11th International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (WORLD COMP '12)	July 16-19, 2012	Paper	Municipal E-Government Security: Insights from Municipalities in Orange County, California
Posters			
Conference Name	**Conference Dates**	**Type**	**Title**
ISOneWorld Conference	April 11-13, 2012	Poster	Municipal E-Government Security: Opportunities and Challenges
25th High Technology Crime Investigation Association (HTCIA) International Conference	Sept. 12-14, 2011	Poster	E-Government Security Concerns for Municipal Government Entities

The feedback, comments and suggestions provided at these conferences were used to:

1) Gauge the level of interest in municipal e-government security.
2) Receive input on findings and conclusions.
3) Serve as a platform to guide future research efforts.

The topic of municipal e-government security and in particular the goals of this study were highly received by the scholarly community at these conferences. While this study provided a vast amount of findings and evidence, it is also clear that the municipal e-government field is still young. While e-government as a whole receives multidisciplinary attention, this study hopes to shed additional focus and attention on the municipal levels of government and the security of their e-government systems.

REFERENCES

Akkaya, C., Obermeier, M., Wolf, P., & Krcmar, H. (2011). Components of Trust Influencing eGovernment Adoption in Germany. In M. Janssen, H. J. Scholl, M. A. Wimmer & Y.-h. Tan (Eds.), *Electronic Government* (Vol. 6846, pp. 88-99). Berlin, Heidelberg: Springer Berlin Heidelberg.

Akkaya, C., Wolf, D. P., & Krcmar, H. (2010, 8/11 to 8/15). *The Role of Trust in E-Government Adoption: A Literature Review.* Paper presented at the 16th Americas Conference on Information Systems (AMCIS 2010), Lima, Peru.

Al-Sobhi, F., Weerakkody, V., & El-Haddadeh, R. (2012). Building Trust in E-Government Adoption through an Intermediary Channel. *International Journal of Electronic Government Research, 8*(2), 91-106.

Alessia C. Neuroni, A. S., Reinhard Riedl. (2010). *Assessing and Evaluating Value and Cost Effectivenes of E-Government Initiatives: Initial Measurement Framework.* Paper presented at the Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Resarch and Pojects of IFIP eGOV and ePart 2010, Lausanne, Switzerland.

Alpar, P., & Olbrich, S. (2005). Legal Requirements and Modelling of Processes in e-Government. *Electronic Journal of e-Government, 3*(3), 107-116.

Andersen, K. V., & Medaglia, R. (2008). eGovernment Front-End Services: Administrative and Citizen Cost-Benefits In M. A. Wimmer, H. J. Scholl & E. Ferro (Eds.), *Electronic Government 7th International Conference, EGOV 2008, Turin, Italy, August 31-September 5, 2008, proceedings* (Vol. 5184/2008, pp. 148-159). Berlin: Springer.

Andresen, K. (2003). For the Good of the Public - What Can We Do For You? Effective Partnering between Local Government and Business for Service Delivery. In R. Traunmüller (Ed.), *Electronic government: Second international conference, EGOV 2003, Prague, Czech Republic, September 2003 : proceedings* (Vol. 2739, pp. 438-441). Berlin / Heidelberg: Springer.

Angelopoulos, S., Kitsios, F., Kofakis, P., & Papadopoulos, T. (2010). Emerging barriers in e-government implementation. In M. A. Wimmer, J.-L. Chappelet, M. Janssen & H. J. Scholl (Eds.), *Electronic Government: 9th IFIP WG 8.5 International Conference, EGOV 2010, Lausanne, Switzerland, Augtust/September 2010: Proceedings* (pp. 216-225). Lausanne, Switzerland: Berlin / Heidelberg.

Anttiroiko, A.-V. (2002). Strategic knowledge management in local government. In Å. Grönlund (Ed.), *Electronic government : design, applications, and management* (pp. 268-298). Hershey, PA: Idea Group Publishing.

Apostolou, D., Mentzas, G., Stojanovic, L., Thoenssen, B., & Lobo, T. P. (2011). A collaborative decision framework for managing changes in e-Government services. *Government Information Quarterly, 28*(1), 101-116. doi: 10.1016/j.giq.2010.03.00

Arabatzis, G., Andreopoulou, Z., Koutroumanidis, T., & Manos, B. (2010). E-Government for Rural Development: Classifying and Ranking Content Characteristics of Development

Agencies Websites. *Journal of Environmental Protection and Ecology, 11*(3), 1138-1149.

Archmann, S., & Nielsen, M. M. (2008). *Interoperability and Its Importance to eGovernment - Success Factors and Barriers*. Paper presented at the 2nd International Conference on Methodologies, Technologies and Tools Enabling e-Government (MeTTeG 2008), Corfu, Greece.

Arendsen, R., & van Engers, T. M. (2004). *Reduction of the Administrative Burden: An e-Government Perspective*. Paper presented at the Electronic Government: 3rd International Conference (EGOV 2004), Berlin / Heidelberg. http://www.springerlink.com/openurl.asp?genre=article&id=BHJ6V5EJU1DW8P1D

Ayyad, M. (2009). *Using the Actor-Network Theory to interpret e-government implementation barriers*. Paper presented at the 3rd International Conference on Theory and Practice of Electronic Governance (ICEGOV 2009), Bogota, Colombia.

Baker, P. M. A., & Bellordre, C. (2004). *Adoption of Information and Communication Technologies: Key Policy Issues, Barriers and Opportunities for People with Disabilities*. Paper presented at the 37th Hawaii International Conference on System Sciences (HICSS-37), Island of Hawaii (Big Island). http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2004/2056/05/2056toc.xml&DOI=10.1109/HICSS.2004.1265319

Bakırlı, G., Birant, D., Mutlu, E., Kut, A., Denktaş, L., & Çetin, D. (2012, 14-15 June). *Data Mining Solutions for Local Municipalities*. Paper presented at the 12th European Conference on eGovernment (ECEG 2012), Barcelona, Spain.

Basu, S. (2007). Legal Issues for E-Government in Developing Countries. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (pp. 1154-1160). Hershey, PA: Idea Group Reference.

Beaumaster, S. (2002). *Local Government IT Implementation Issues: A Challenge for Public Administration*. Paper presented at the 35th Hawaii International Conference on System Sciences (HICSS-35), Island of Hawaii (Big Island). http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2002/1435/05/1435toc.xml&DOI=10.1109/HICSS.2002.994084

Becker, J., Hofmann, S., & Räckers, M. (2011). Coverage of eGovernment Security Issues in Mass Media. In M. Janssen, H. J. Scholl, M. A. Wimmer & Y.-h. Tan (Eds.), *Electronic Government* (Vol. 6846, pp. 296-307). Berlin, Heidelberg: Springer Berlin Heidelberg.

Becker, S. A. (2005). Potential trust barriers in US state e-government privacy policies. *Electronic Government: An International Journal, 2*(3), 334-352.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. [doi: DOI: 10.1016/j.jsis.2007.12.002]. *The Journal of Strategic Information Systems, 17*(2), 165-176.

Belanger, F., & Hiller, J. S. (2006). A framework for e-government: privacy implications. *Business Process Management Journal, 12*, 48-60.

Berghmans, P., & Van Roy, K. (2011). Information Security Risks in Enabling e-Government: The Impact of IT Vendors. *Information Systems Management, 28*(4), 284-293. doi: 10.1080/10580530.2010.514212

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2012). Promoting transparency and accountability through ICTs, social media, and collaborative e-government. *Transforming Government: People, Process and Policy, 6*(1), 78-91.

Beynon-Davies, P. (2007). Models for e-government. *Transforming Government: People, Process and Policy, 1*(1), 7-28.

Bonsón, E., Torres, L., Royo, S., & Flores, F. (2012). Local e-government 2.0: Social media and corporate transparency in municipalities. *Government Information Quarterly, 29*(2), 123-132.

Brechbuhl, H. B., Robert; Dynes, Scott; Johnson, M. Eric. (2010). Protecting Critical Information Infrastructure: Developing Cybersecurity Policy. *Information Technology for Development, 16*(1), 83-91.

Brown, M. M. (2000). Mitigating the Risk of Information Technology Initiatives: Best Practices and Points of Failure for the Public Sector. In G. D. Garson (Ed.), *Handbook of Public Information Systems* (pp. 153-164). New York: Marcel Dekker.

Brown, M. M. (2001). The Benefits and Costs of Information Technology Innovations: An Empirical Assessment of a Local Government Agency. *Pubic Performance & Management Review, 24*(4), 351 - 366.

Brunschwig, C. (2002). *Legal Design and e-Government: Visualisations of Cost &amp; Efficiency Accounting in the e-Learning Environment of the Canton of Zurich (Switzerland)*. Paper presented at the Electronic government: First international conference, EGOV 2002, Aix-en-Provence, France, September 2-6, 2002 : proceedings, Berlin / Heidelberg. http://www.springerlink.com/openurl.asp?genre=article&id=29T6M2XVU0D44ADH

Carter, L., & Bélanger, F. (2005a). The utilization of e-government services: citizen trust, innovation and acceptance factors. [Article]. *Information Systems Journal, 15*(1), 5-25. doi: 10.1111/j.1365-2575.2005.00183.x

Carter, L., & Bélanger, F. (2005b). The utilization of e-government services: citizen trust, innovation and acceptance factors *. *Information Systems Journal, 15*(1), 5-25.

Castelnovo, W., & Simonetta, M. (2007). The Evaluation of e-Government Projects for Small Local Government Organisation. *Electronic Journal of e-Government, 5*(1), 21-28.

Caudle, S. L. (1990). Managing Information Resources in State Government. [Article]. *Public Administration Review, 50*(5), 515-524.

Caudle, S. L., Gorr, W. L., & Newcomer, K. E. (1991). Key Information Systems Management Issues for the Public Sector. [Article]. *MIS Quarterly, 15*(2), 171-188.

Chen, X., Kong, W., & Futatsugi, K. (2007). *Formal Support for e-Government System Design with Transparency Consideration*. Paper presented at the 1st International Conference on Theory and Practice of Electronic Governance (ICEGOV 2007), Macao.

Chen, Y.-S., Chong, P. P., & Zhang, B. (2004). Cyber security management and e-government. *Electronic Government: An International Journal, 1*(3), 316-327.

Chissick, M., Harrington, J., & Azhar, L. (2004). *E-government : a practical guide to the legal issues*. London: Sweet & Maxwell.

Choudrie, J., Raza, S., & Olla, P. (2009). *Exploring the Issues of Security, Privacy and Trust in eGovernment: UK Citizens' Perspective*. Paper presented at the 15th Americas Conference on Information Systems (AMCIS 2009), San Francisco, CA. http://aisel.aisnet.org/amcis2009/347

Chourabi, H., Mellouli, S., & Bouslama, F. (2009). Modeling e-government business processes: New approaches to transparent and efficient performance *Information Polity, 14*(1-2), 91-109. doi: 10.3233/IP-2009-0168

Chutimaskul, W., Funilkul, S., & Chongsuphajaisiddhi, V. (2008). *The quality framework of e-government development.* Paper presented at the Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance, Cairo, Egypt.

Ciborra, C. (2005). Interpreting e-government and development: Efficiency, transparency or governance at a distance? *Information Technology & People, 18*(3), 260-279.

Cohen, J. E. (2006). Citizen satisfaction with contacting government on the internet. *Information Polity: The International Journal of Government & Democracy in the Information Age, 11*(1), 51-65.

Conklin, A., & White, G. (2006). e-Government and Cyber Security: The Role of Cyber Security Exercises.

Conklin, A., & White, G. B. (2006). *e-Government and Cyber Security: The Role of Cyber Security Exercises.* Paper presented at the 39th Hawaii International Conference on System Sciences (HICSS-39), Kauai. http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2006/2507/04/25074toc.xml&DOI=10.1109/HICSS.2006.133

Conklin, W. (2007). Barriers to Adoption of e-Government.

Conklin, W. A. (2007). *Barriers to Adoption of E-Government.* Paper presented at the 40th Hawaii International Conference on System Sciences (HICSS-40), Waikoloa, Big Island, HI.

Cook, M. E., LaVigne, M. F., Pagano, C. M., Dawes, S. S., & Pardo, T. A. (2002). Making a Case for Local E-Government (pp. 1-16). Albany, NY: Center for Technology in Government.

Cordella, A., & Iannacci, F. (2010). Information systems in the public sector: The e-Government enactment framework. [doi: DOI: 10.1016/j.jsis.2010.01.001]. *The Journal of Strategic Information Systems, 19*(1), 52-66.

Coursey, D., & Norris, D. F. (2008). Models of E-Government: Are They Correct? An Empirical Assessment. [Article]. *Public administration review, 68*(3), 523-536. doi: 10.1111/j.1540-6210.2008.00888.x

Crichton, C., Davies, J., Gibbons, J., Harris, S., & Shukla, A. (2007). *Semantic frameworks for e-government.* Paper presented at the Proceedings of the 1st international conference on Theory and practice of electronic governance, Macao, China.

Dae-Ho Byun, G. F. (2011). Evaluating usability, user satisfaction and intention to revisit for successful e-government websites. *Electronic Government, an International Journal, 8*(1), 1-19.

Das, J., DiRienzo, C., & Burbridge, J., John. (2009). Global E-Government and the Role of Trust: A Cross Country Analysis. *International Journal of Electronic Government Research, 5*(1), 1-18.

Dawes, S. (2008). *An exploratory framework for future E-Government research investments.*

Dawes, S. S., & Helbig, N. (2010). Information strategies for open government: challenges and prospects for deriving public value from government transparency. In M. A. Wimmer, J.-L. Chappelet, M. Janssen & H. J. Scholl (Eds.), *Electronic Government:*

9th IFIP WG 8.5 International Conference, EGOV 2010, Lausanne, Switzerland, Augtust/September 2010: Proceedings (pp. 50-60). Berlin / Heidelberg: Springer-Verlag.

Decman, M., & Klun, M. (2010, June 17 -18). *The Path to Administrative Burden Reduction – With the Help of IT: Challenges and Opportunities in Slovenia.* Paper presented at the 10th European Conference on e-Government (ECEG 2010), University of Limerick, Ireland.

dos Santos, E. M., & Reinhard, N. (2010, 8/11 to 8/15). *Barriers to Government Interoperability Frameworks Adoption.* Paper presented at the 16th Americas Conference on Information Systems (AMCIS 2010), Lima, Peru.

dos Santos, E. M., & Reinhard, N. (2012). Electronic Government Interoperability: Identifying the Barriers for Frameworks Adoption. *Social Science Computer Review, 30*(1), 71-82. doi: 10.1177/0894439310392196

Dutton, W., Guerra, G. A., Zizzo, D. J., & Peltu, M. (2005). The cyber trust tension in E-government: Balancing identity, privacy, security. *Information Polity: The International Journal of Government & Democracy in the Information Age, 10*(1,2), 13-24.

Ebrahim, Z., & Irani, Z. (2005a). E-government adoption: architecture and barriers. *Business Process Management Journal, 11*(5).

Ebrahim, Z., & Irani, Z. (2005b). E-government adoption: architecture and barriers. *Business Process Management Journal, 11*(5), 589-611.

Edmiston, K. D. (2003). State and local e-government: Prospects and challenges. *American Review of Public Administration, 33*(1), 20-45.

Eyob, E. (2004). E-government: breaking the frontiers of inefficiencies in the public sector. *Electronic Government: An International Journal, 1*(1), 107-114.

Eyob, E. (2007). Evaluating Methodologies of Financial Cost and Benefit Aspects of E-Government. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (Vol. 1, pp. 784-789). Hershey, PA: Idea Group Reference.

Faisal, M. N., & Rahman, Z. (2008). E-government in India: modelling the barriers to its adoption and diffusion. *Electronic Government: An International Journal, 5*(2), 181-202.

Fenster, M. (2012). Disclosure's Effects: WikiLeaks and Transparency. *Iowa Law Review, 97*(3), 753-807.

Fiedler, G., & Schmidt, P. (2005). *Developing Interactive Voice Response Interfaces for Large Information Systems.* Paper presented at the 1st European Mobile Government Conference (Euro mGov 2005), Brighton, UK.

Fogli, D., Colosio, S., & Sacco, M. (2010). Managing accessibility in local e-government websites through end-user development: a case study. *Universal Access in the Information Society, 9*(1), 35-50.

Galindo, F. (2002). e-Government Trust Providers. In Å. Grönlund (Ed.), *Electronic Government: Design, Applications, and Management* (pp. 121-150). Hershey, PA: IDEA Group Publishing.

Gefen, D., Warkentin, M., Pavlou, P. A., & Rose, G. M. (2002). *E-Government adoption.* Paper presented at the 8th Americas Conference on Information Systems (AMCIS 2002), Dallas, TX.

Gertraud Peinel, M. J., Thomas Rose (2010). Business models for eGovernment services. *Electronic Government, an International Journal, 7*(3), 380 - 401.

Gil-Garcia, J. R., & Luna-Reyes, L. F. (2003). Towards a Definition of Electronic Government: A Comparative Review. In A. Mendez-Vilas, J. A. Mesa Gonzalez, J. Mesa Gonzalez, V. Guerrero Bote & F. Zapico Alonso (Eds.), *Techno-legal Aspects of the Information Society and New Economy: An Overview* (pp. 102-108). Badajoz, Spain: Formatex.

Gil-Garcia, J. R., & Martinez-Moyano, I. J. (2007). Understanding the evolution of e-government: The influence of systems of rules on public sector dynamics. [doi: DOI: 10.1016/j.giq.2006.04.005]. *Government Information Quarterly, 24*(2), 266-290.

Gilbert, D., Balestrini, P., & Littleboy, D. (2004). Barriers and benefits in the adoption of e-government. *The International Journal of Public Sector Management, 17*(4/5), 286-301.

Glassey, O. (2004). Developing a one-stop government data model. [doi: DOI: 10.1016/j.giq.2003.12.012]. *Government Information Quarterly, 21*(2), 156-169.

Grant, G., & Chau, D. (2005). Developing a Generic Framework for E-Government. *Journal of Global Information Management, 13*(1), 1-30.

Grimmelikhuijsen, S. (2012). Linking transparency, knowledge and citizen trust in government: an experiment. *International Review of Administrative Sciences, 78*(1), 50-73. doi: 10.1177/0020852311429667

Grönlund, Å. (2002). Electronic Government: Efficiency, Service Quality, and Democracy. In Å. Grönlund (Ed.), *Electronic government : design, applications, and management* (pp. 23 - 50). Hershey, PA: Idea Group Publishing.

Grönlund, Å., & Horan, T. A. (2005). Introducing e-Gov: History, Definitions, and Issues. *Communications of the Association for Information Systems, 15*(39), 713-729.

Gupta, M., & Jana, D. (2003). E-government evaluation: A framework and case study. *Government Information Quarterly, 20*(4), 365-387.

Hadzilias, E. A. (2005). A Methodology Framework for Calculating the Cost of e-Government Services. In M. Böhlen, J. Gamper, W. Polasek & M. A. Wimmer (Eds.), *E-Government: Towards Electronic Democracy* (Vol. 3416, pp. 247-256). Berlin / Heidelbert: Springer.

Halaris, C., Magoutas, B., Papadomichelaki, X., & Mentzas, G. (2007). Classification and synthesis of quality approaches in e-government services. *Internet Research, 17*(4), 378-401.

Halchin, L. E. (2004). Electronic government: Government capability and terrorist resource. [doi: DOI: 10.1016/j.giq.2004.08.002]. *Government Information Quarterly, 21*(4), 406-419.

Hazlett, S.-A., & Hill., F. (2003). E-government: the realities of using IT to transform the public sector. *Managing Service Quality, 13*(6), 445-452.

Helbig, N., Styrin, E., Canestraro, D., & Pardo, T. (2010). *Information and transparency: learning from recovery act reporting experiences*. Paper presented at the 11th Annual International Conference on Digital Government Research (dg.o 2010), Puebla, Mexico.

Ho, A. T.-K. (2002). Reinventing Local Governments and the E-Government Initiative. [Article]. *Public Administration Review, 62*(4), 434-444.

Hof, S. (2003). Security Aspects within e-Government. In R. Traunmüller (Ed.), *Electronic government: Second international conference, EGOV 2003, Prague, Czech Republic, September 2003 : proceedings* (Vol. 2739, pp. 266-271). Berlin / Heidelberg: Springer.

Hofmann, S., & Heierhoff, L. (2012, 9-11 August). *Adoption of Municipal e-Government Services – A Communication Problem?* Paper presented at the 18th Americas Conference on Information Systems (AMCIS 2012), Seattle, Washington, USA.

Holden, S. H., Norris, D. F., & Fletcher, P. D. (2003). Electronic government at the local level: Progress to date and future issues. *Public Performance & Management Review, 26*(4), 325-344.

Horsburgh, S., Goldfinch, S., & Gauld, R. (2011). Is Public Trust in Government Associated With Trust in E-Government? *Social Science Computer Review, 29*(2), 232-241. doi: 10.1177/0894439310368130

Hsu, F.-M., Lin, Y.-T., Fang, C.-T., & Chiu, C.-M. (2012, 11-15 July). *A framework for users' satisfaction of information systems in e-government.* Paper presented at the 16th Pacific Asia Conference on Information Systems (PACIS 2012), Ho Chi Minh City, Vietnam.

Huijboom, N., & Hoogwout, M. (2004). *Trust in e-Government Cooperation.* Paper presented at the Electronic Government: 3rd International Conference (EGOV 2004), Berlin / Heidelberg. http://www.springerlink.com/openurl.asp?genre=article&id=LWLNF7H7UPCGQXCH

Iglesias, S. A. a. J. C. (2010, July 1-2, 2010). *Towards A More Effective And Efficient EGovernment: The Importance Of Shared Service.* Paper presented at the 4th International Conference on Methodologies, Technologies and Tools enabling e-Government (MeTTeG 2010), Olten, Switzerland.

Jain, V., & Kesar, S. (2008). *E-Government Implementation Challenges at Local Level: A Citizens' Centric Perspective.* Paper presented at the 14th Americas Conference on Information Systems (AMCIS 2008), Toronto, ON.

Jain, V., & Kesar, S. (2011). E-government implementation challenges at local level: a comparative study of government and citizens' perspectives. *Electronic Government, an International Journal, 8*(2/3), 208 - 225.

Janssen, M., Kuk, G., & Wagenaar, R. W. (2005). *A survey of e-government business models in the Netherlands.* Paper presented at the 7th International Conference on Electronic Commerce (ICEC 2005), Xi'an, China.

Joha, A., & Janssen, M. (2011, 12-15 June 2011). *Types of shared services business models in public administration.* Paper presented at the 12th Annual International Conference on Digital Government Research (dg.o 2011), College Park, MD, USA.

Joshi, J. B. D., Ghafoor, A., Aref, W. G., & Spafford, E. H. (2002). Security and Privacy Challenges of a Digital Government. In W. J. McIver, Jr. & A. K. Elmagarmid (Eds.), *Advances in Digital Government. Technology, Human Factors, and Policy* (pp. 121-136). Norwell, MA: Kluwer Academic Publishers.

Joshi, J. B. D., Joshi, S. R., & Chandran, S. M. (2007). Information Security Issues and Challenges. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (pp. 1047-1053). Hershey, PA: Idea Group Reference.

Jun, K.-N., & Weare, C. (2008). *The Adoption of Municipal Web Sites: On Efficiency, Power, and Legitimacy*. Paper presented at the 9th Annual International Conference on Digital Government Research (dg.o 2008), Montreal, Canada.

Kaaya, J. (2009). Determining Types of Services and Targeted Users of Emerging E-Government Strategies: The Case of Tanzania. *International Journal of Electronic Government Research, 5*(2), 16-36.

Kaliontzoglou, A., Sklavos, P., Karantjias, T., & Polemi, D. (2005). A secure e-Government platform architecture for small to medium sized public organizations. [doi: DOI: 10.1016/j.elerap.2004.09.002]. *Electronic Commerce Research and Applications, 4*(2), 174-186.

Khayyat, N. T. (2010). Effects of Information Technology on Cost, Quality and Efficiency in Provision of Public Services. *Information and Communication Technologies Policies and Practices*, 73-90.

Kim, H. J., & Bretschneider, S. (2004). *Local Government Information Technology Capacity: An Exploratory Theory*. Paper presented at the 37th Hawaii International Conference on System Sciences (HICSS-37), Island of Hawaii (Big Island). http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2004/2056/05/2056toc.xml&DOI=10.1109/HICSS.2004.1265310

Kiskis, M., & Petrauskas, R. (2003). e-Governance: Two Views on Legal Environment. In R. Traunmüller (Ed.), *Electronic government: Second international conference, EGOV 2003, Prague, Czech Republic, September 2003 : proceedings* (Vol. 2739, pp. 407-412). Berlin / Heidelberg: Springer.

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. [doi: DOI: 10.1016/j.cose.2006.08.004]. *Computers & Security, 25*(7), 522-538.

Koerkner, C. (2011). Hackers threaten Fullerton police website, email, *Orange County Register*. Retrieved from http://www.ocregister.com/articles/police-312020-officers-anonymous.html

Kostresevic, M., & Simic, D. (2011). Security measures for protection of e-Government IT infrastructure. *Technics Technologies Education Management-Ttem, 6*(3), 801-810.

Kumar, R. (2010). *Research methodology: A step-by-step guide for beginners*: Sage Publications Limited.

Lam, W. (2005). Barriers to e-government integration. *Journal of Enterprise Information Management, 18*(5), 511-530. doi: 10.1108/17410390510623981

LaVoy, D. F. (2001). Trust and reliability. *Public Manager, 30*(3), 8.

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*(2), 122-136.

Lee, J., Lee, H., & Kim, T. (2012, 3-5 July). *Evaluating and Assessing a Typology of Ubiquitous City Services by Classifying and Assigning Actual Services from an Inventory of Identified Services*. Paper presented at the 6th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2012), Abany, New York.

Lee, J., Oh, K.-T., & Kwon, H. Y. (2008). *Striving for transparency and efficiency in e-government: procurement reform through e-procurement*. Paper presented at the 2nd

International Conference on Theory and Practice of Electronic Governance (ICEGOV 2008), Cairo, Egypt.

Levack, K. (2003). The E-Government Act of 2002: A stab at cyber security. *Econtent, 26*(3), 8-+.

Li, Y. (2011, 4-7 August 2011). *Developing a Dichotomy of Information Privacy Concerns.* Paper presented at the 17th Americas Conference on Information Systems (AMCIS 2011), Detroit, MI, USA.

Loukis, E., & Tavlaki, E. (2007). Electronic Business Models Design for Public-Private Partnerships. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (Vol. 1, pp. 615-623). Hershey, PA: Idea Group Reference.

Luna-Reyes, L. F., & Gil-Garcia, J. R. (2003). *E-Government Security, Privacy and Information Access: Some Policy and Organizational Trade-offs*. Paper presented at the International Conference on Public Participation and Information Technologies 2003 (ICPPIT03), Cambridge, MA.

Magoutas, B., & Mentzas, G. (2009). Refinement, Validation and Benchmarking of a Model for E-Government Service Quality. In M. A. Wimmer, H. J. Scholl, M. Janssen & R. Traunmüller (Eds.), *Electronic Government: 8th International Conference (EGOV 2009)* (Vol. 5693, pp. 139-150). Berlin: Springer Verlag.

Mann, H., Grant, G., & Mann, I. (2011). City E-Government: Scope and its Realization. *International Journal of Electronic Government Research, 7*(1), 38-50.

Marchionini, G., Samet, H., & Brandt, L. (2003). Digital Government. [Article]. *Communications of the ACM, 46*(1), 24-27.

Marques, F., Dias, G. P., & Zuquete, A. (2009). *Security Concerns in E-Government Agent-Based Interoperability.* Paper presented at the Proceedings of ongoing research, general development issues and projects of EGOV 09 8th International Conference, Linz, Austria.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: a structured methodology*. New York: Auerbach Publications.

McLeod Jr., A. J., & Pippin, S. E. (2009). *Security and Privacy Trust in E-Government: Understanding System and Relationship Trust Antecedents*. Paper presented at the 42nd Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, Big Island, Hawaii.

Meneklis, V., & Douligeris, C. (2010). Bridging theory and practice in e-government: A set of guidelines for architectural design. [doi: DOI: 10.1016/j.giq.2009.08.005]. *Government Information Quarterly, 27*(1), 70-81.

Mitrakas, A., Hengeveld, P., Polemi, D., & Gamper, J. (2007). Secure eGovernment Web Services. *Information Technology Newsletter, 18*(1), 21.

Moon, M. J., & Norris, D. F. (2005). Does managerial orientation matter? The adoption of reinventing government and e-government at the municipal level. [Article]. *Information Systems Journal, 15*(1), 43-60. doi: 10.1111/j.1365-2575.2005.00185.x

Mosse, B., & Whitley, E. A. (2009). Critically classifying: UK e-government website benchmarking and the recasting of the citizen as customer. *Information Systems Journal, 19*(2), 149-173. doi: 10.1111/j.1365-2575.2008.00299.x

Myers, M. (1997). Qualitative research in information systems. *MIS Quarterly, 21*(2), 241-242.

Myers, M. D. (2009). *Qualitative Research in Business and Management*. Thousand Oaks: Sage Publications Inc.

Navarrete, C. (2010, 5-8 January 2010). *Trust in E-Government Transactional Services: A Study of Citizens' Perceptions in Mexico and the U.S.* Paper presented at the 43rd Hawaii International Conference on System Sciences (HICSS-43), Koloa, Kauai, HI.

Norris, D., & Reddick, C. (2012, 14-15 June). *eGovernment Among US Local Governments: Current Status and Recent Trends.* Paper presented at the 12th European Conference on eGovernment (ECEG 2012), Barcelona, Spain.

Nour, M. A., AbdelRahman, A. A., & Fadlalla, A. (2008). A context-based integrative framework for e-government initiatives. [doi: DOI: 10.1016/j.giq.2007.02.004]. *Government Information Quarterly, 25*(3), 448-461.

Olbrich, S. (2010, 8/11 to 8/15). *Towards interoperable E-Government – identifying and classifying G2B services in the European metropolitan area Rhine-Neckar.* Paper presented at the 16th Americas Conference on Information Systems (AMCIS 2010), Lima, Peru.

Orlikowski, W., & Baroudi, J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.

Ostermann, H., & Staudinger, R. (2007). Corruption, Transparency, and E-Government. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (Vol. 1, pp. 251-259). Hershey, PA: Idea Group Reference.

Panagiotopoulos, P., Al-Debei, M. M., Fitzgerald, G., & Elliman, T. (2012). A business model perspective for ICTs in public engagement. *Government Information Quarterly, 29*(2), 192-202.

Paolo, G., Massacci, F., & Zannone, N. (2007). *E-Government and On-line Services: Security and Legal Patterns.* Paper presented at the 1st International Conference on Methodologies, Technologies and Tools Enabling e-Government (MeTTeG 2007), Camerino, Italy.

Parent, M., Vandebeek, C., & Gemino, A. (2005). Building citizen trust through e-government. *Government Information Quarterly, 22*(4), 720-736.

Parent, M., Vandebeek, C. A., & Gemino, A. C. (2005). Building Citizen Trust Through E-government. *Government Information Quarterly, 22*(4), 720-736.

Penprase, M. (2012). City of Springfield website restored after hack, *News Leader*. Retrieved from http://www.news-leader.com/article/20120322/NEWS01/303210083/City-website-fully-functional-Springfield

Piotrowski, S. J., & Borry, E. L. (2009). Transparency and Local Government Websites. In C. G. Reddick (Ed.), *Handbook of Research on Strategies for Local E-Government Adoption and Implementation: Comparative Studies* (Vol. 1, pp. 390-407). Hershey, PA; London, UK: Information Science Reference.

Pipe, R. (2006). Breaking Barriers to e-Government. *I-Ways, 29*(4), 164-164.

Premkumar, G., Ho, A. T., & Chakraborty, P. (2006). E-government evolution: an evaluation of local online services. *International Journal of Electronic Business, 4*(2), 177-190.

Raus, M., Liu, J., & Kipp, A. (2010). Evaluating IT innovations in a business-to-government context: A framework and its applications. [doi: DOI: 10.1016/j.giq.2009.04.007]. *Government Information Quarterly, 27*(2), 122-133.

Reddick, C. G. (2005). Empirical Models of E-Government Growth in Local Governments. *e-Service Journal, 3*(2), 59-84.

Relyea, H. C., & Hogue, H. B. (2004). A Brief History of the Emergence of Digital Government in the United States. In A. Pavlichev & G. D. Garson (Eds.), *Digital Government: Principles and Best Practices* (pp. 16-33). Hershey: Idea Publishing Group.

Rice, M. F., Alsobrook, R. A., & Weinberger, G. M. (1982). Computer Security in Small Local Governments in Texas. *Texas Business Review, 56*(2), 100.

Richards, M., Adam, K., & Price, B. A. (2005). *It's Okay To Be A Dog On The Internet – Privacy And Trust In e-Government.* Paper presented at the 1st European Mobile Government Conference (Euro mGov 2005), Brighton, UK.

Rowe, N. C. (2007). Trust in Digital Government. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (pp. 1572-1576). Hershey, PA: Idea Group Reference.

Roy, J. (2005). Service, Security, Transparency & Trust: Government Online or Governance Renewal in Canada? *International Journal of Electronic Government Research, 1*(1), 40-58.

Saarenpää, A. (2003). A Legal Framework for e-Government. In R. Traunmüller (Ed.), *Electronic government: Second international conference, EGOV 2003, Prague, Czech Republic, September 2003 : proceedings* (Vol. 2739, pp. 377-384). Berlin / Heidelberg: Springer.

Sarantis, D., Charalabidis, Y., & Askounis, D. (2011). A goal-driven management framework for electronic government transformation projects implementation. *Government Information Quarterly, 28*(1), 117-128. doi: 10.1016/j.giq.2009.10.006

Scherlis, W. L., & Eisenberg, J. (2003). IT Research, Innovation, and E-Government. [Article]. *Communications of the ACM, 46*(1), 67-68.

Scholl, H. J. (2003). *E-government: A Special Case of ICT-enabled Business Process Change.* Paper presented at the 36th Hawaii International Conference on System Sciences (HICSS-36), Island of Hawaii (Big Island). http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2003/1874/05/1874toc.xml&DOI=10.1109/HICSS.2003.10015

Scholl, H. J. (2006). *What can e-Commerce and e-Government learn from each other?* Paper presented at the Proceedings of the 2006 international conference on Digital government research, San Diego, California.

Schwester, R. W. (2009). Examining the Barriers to e-Government Adoption. *Electronic Journal of e-Government, 7*(1), 113-122.

Seifert, J. W., & Relyea, H. C. (2007). E-Government Act of 2002 in the United States. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (Vol. 1, pp. 476-481). Hershey, PA: Idea Group Reference.

Sell, A., Patokorpi, E., & Walden, P. (2006). Enhancing Public Sector Service Efficiency by Electronic Commerce *Electronic Journal of e-Government, 4*(1), 37-48.

Shackleton, P., Fisher, J., & Dawson, L. (2004). *Evolution of Local Government E-Services: The Applicability of E-Business Maturity Models.* Paper presented at the 37th Hawaii International Conference on System Sciences (HICSS-37), Island of Hawaii (Big Island). http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss

/&toc=comp/proceedings/hicss/2004/2056/05/2056toc.xml&DOI=10.1109/HICSS.2004.1265308

Si, H., & Li, C.-T. (2007). Maintaining Information Security in E-Government through Steganology. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (pp. 1180-1184). Hershey, PA: Idea Group Reference.

Smith, M. L. (2010). Building institutional trust through e-government trustworthiness cues. *Information Technology & People, 23*(3), 222-246. doi: Doi 10.1108/09593841011069149

Stamoulis, D., Gouscos, D., Georgiadis, P., & Martakos, D. (2001). Revisiting public information management for effective e-government services. *Information Management & Computer Security, 9*(4), 146-153.

Stibbe, M. (2005). E-government security. *Infosecurity Today, 2*(3), 8-10.

Taylor, G. (2002). Computer rules for network security. *The American City & County, 117*(12).

Thomas, J. C., & Streib, G. (2003). The New Face of Government: Citizen-Initiated Contacts in the Era of E-Government. [Article]. *Journal of Public Administration Research & Theory, 13*(1), 83.

Thomson, J. D. (2011, 16-17 June 2011). *An Efficient, Effective eGovernment Enterprise Resource Planning Model.* Paper presented at the 11th European Conference on eGovernment (ECEG 2011), Ljubljana, Slovenia.

Tolbert, C., & Mossberger, K. (2003). *The effects of e-government on trust and confidence in government.* Paper presented at the Proceedings of the 2003 annual national conference on Digital government research, Boston, MA.

Tolbert, C. J., & Mossberger, K. (2006). The Effects of E-Government on Trust and Confidence in Government. *Public Administration Review, 66*(3), 354-369.

van Veenstra, A. F., Klievink, B., & Janssen, M. (2009, June 8-10, 2009). *Barriers for transformation: Impediments for transforming the public sector through e-government.* Paper presented at the 17th European Conference on Information Systems (ECIS 2009), Verona, Italy.

van Velsen, L., van der Geest, T., ter Hedde, M., & Derks, W. (2009). Requirements engineering for e-Government services: A citizen-centric approach and case study. [doi: DOI: 10.1016/j.giq.2009.02.007]. *Government Information Quarterly, 26*(3), 477-486.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of information systems, 4*(2), 74-81.

Wang, J. (2009). *E-government Security Management: Key Factors and Countermeasure.*

Welch, E. W. (2005). Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory, 15*(3), 371-391.

Welch, E. W., & Hinnant, C. C. (2003). *Internet Use, Transparency, and Interactivity Effects on Trust in Government.* Paper presented at the 36th Hawaii International Conference on System Sciences (HICSS-36), Island of Hawaii (Big Island). http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2003/1874/05/1874toc.xml&DOI=10.1109/HICSS.2003.1174323

Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with e-government and trust in government. [Article]. *Journal of Public Administration Research & Theory, 15*(3), 371.

West, D. M. (2004). E-Government and the Transformation of Service Delivery and Citizen Attitudes. [Article]. *Public Administration Review, 64*(1), 15-27. doi: 10.1111/j.1540-6210.2004.00343.x

Wilson, S. C. (2012, 4-7 June). *e-government legislation meets the poverty threshold: issues for the economically disadvantaged.* Paper presented at the 13th Annual International Conference on Digital Government Research (dg.o '12), College Park, MD.

Wimmer, M., & von Bredow, B. (2002). *A Holistic Approach to Security Aspects in E-government.* Paper presented at the 35th Hawaii International Conference on System Sciences (HICSS-35), Island of Hawaii (Big Island). http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2002/1435/05/1435toc.xml&DOI=10.1109/HICSS.2002.994083

Winkel, O. (2007). Electronic government and network security: a viewpoint. *Transforming Government: People, Process and Policy, 1*(3), 220-229.

Wittmann, G., Breitschaft, M., Krabichler, T., & Stahl, E. (2007). *Selection of Appropriate Payment Methods for E-Government – Model and Application.* Paper presented at the Electronic Government: 6th International Conference, (EGOV 2007), Regensburg, Germany. http://www.springerlink.com/content/c7675k1211205155/?p=ac4060cfea1d479bbe5f362e481b9e46&pi=16

Wohlers, T. E. (2007). *Comparative E-Government: Trends and Sophistication at the Local Level.* Paper presented at the Conference Papers -- Midwestern Political Science Association.

Wohlers, T. E. (2010). Local E-Government Sophistication in the United States. In H. J. Scholl (Ed.), *E-Government: Information, Technology, and Transformation* (Vol. 17, pp. 89-105). Armonk, NY: M.E. Sharpe.

Wyld, D. C. (2004). The 3 Ps: The Essential Elements of a Definition of E-Government. *Journal of E-Government, 1*(1), 17-22.

Yadav, N., & Yadav, H. (2009). An electronic government model based on case study approach. *Electronic Government, an International Journal, 6*(4), 421-432. doi: 10.1504/EG.2009.027787

Yarlagadda, P., & Ahmed, S. (2007). *Efficiency of Electronic Public Service Delivery in India: Public-Private Partnership as a Critical Factor* Paper presented at the 1st International Conference on Theory and Practice of Electronic Governance (ICEGOV 2007), Macao.

Yee, G., El-Khatib, K., Korba, L., Patrick, A. S., Song, R., & Xu, Y. (2005). Privacy and Trust in E-Government. In W. Huang, K. Siau & K. K. Wei (Eds.), *Electronic Government Strategies and Implementation* (pp. 145-190). Hershey, PA: Idea Group Publishing.

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5): Sage publications, INC.

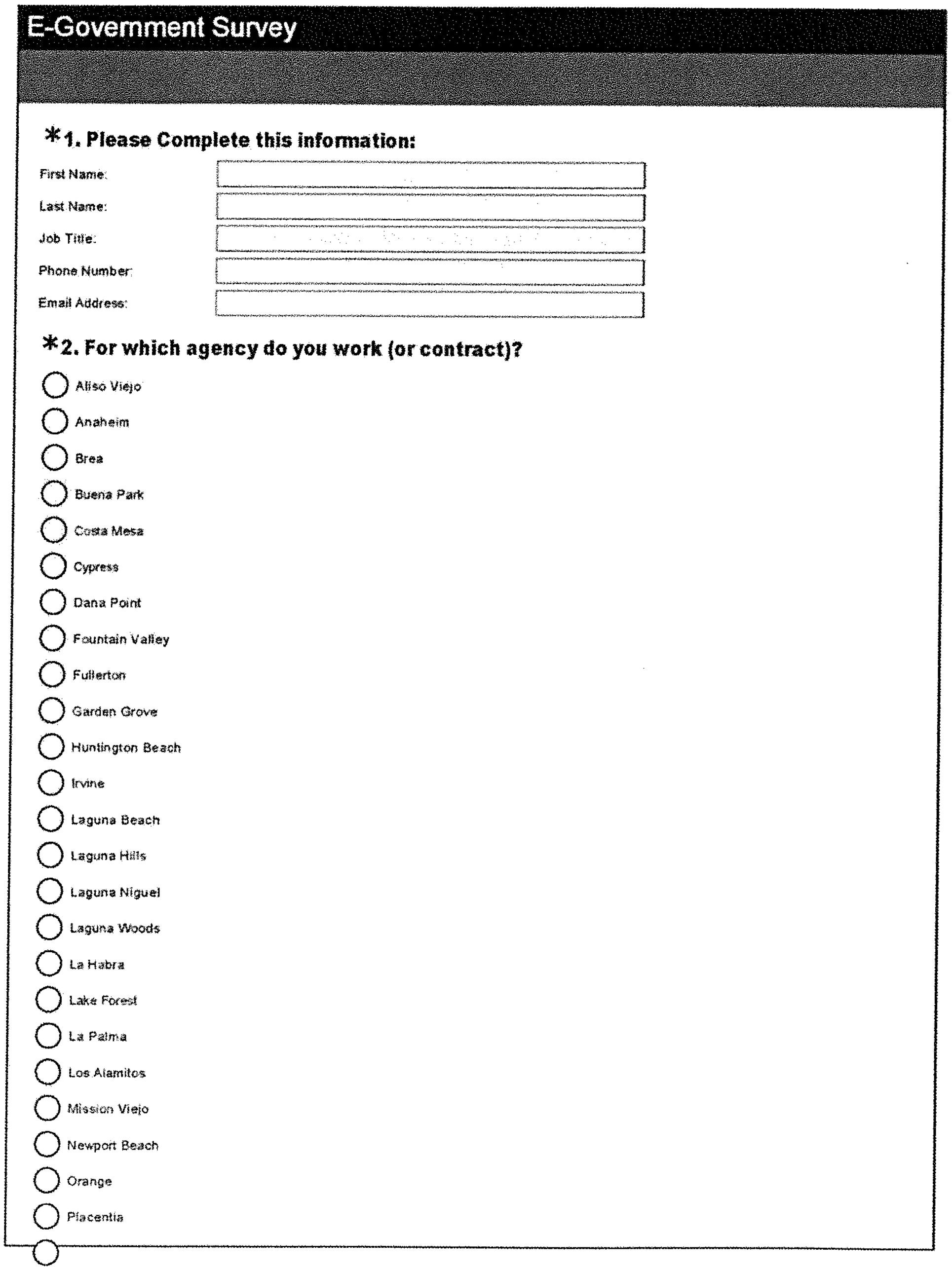
Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. [doi: DOI: 10.1016/j.giq.2009.07.004]. *Government Information Quarterly, 27*(1), 49-56.

Zhou, P. (2008). *An Adaptive Framework for Managing Knowledge in E-Government.*

Zinnbauer, D. (2007). Transparency and Information Disclosure in E-Government. In A.-V. Anttiroiko & M. Mälkiä (Eds.), *Encyclopedia of digital government* (pp. 1566-1571). Hershey, PA: Idea Group Reference.

APPENDICES

APPENDIX A: PRE-INTERVIEW PARTICIPANT SURVEY QUESTIONS



E-Government Survey

*1. Please Complete this information:

First Name:

Last Name:

Job Title:

Phone Number:

Email Address:

*2. For which agency do you work (or contract)?

○ Aliso Viejo

○ Anaheim

○ Brea

○ Buena Park

○ Costa Mesa

○ Cypress

○ Dana Point

○ Fountain Valley

○ Fullerton

○ Garden Grove

○ Huntington Beach

○ Irvine

○ Laguna Beach

○ Laguna Hills

○ Laguna Niguel

○ Laguna Woods

○ La Habra

○ Lake Forest

○ La Palma

○ Los Alamitos

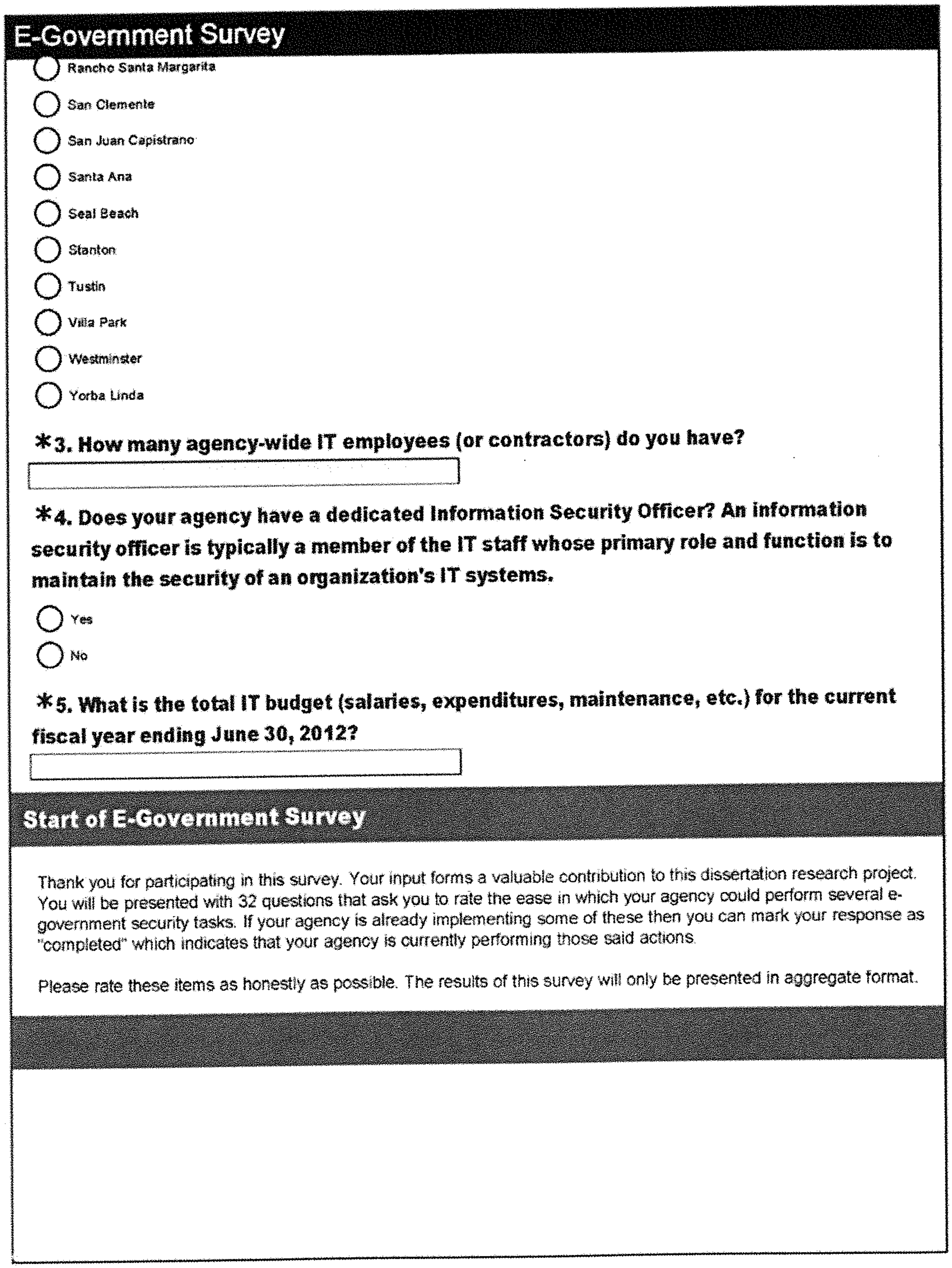
○ Mission Viejo

○ Newport Beach

○ Orange

○ Placentia

○



E-Government Survey

○ Rancho Santa Margarita

○ San Clemente

○ San Juan Capistrano

○ Santa Ana

○ Seal Beach

○ Stanton

○ Tustin

○ Villa Park

○ Westminster

○ Yorba Linda

***3. How many agency-wide IT employees (or contractors) do you have?**

***4. Does your agency have a dedicated Information Security Officer? An information security officer is typically a member of the IT staff whose primary role and function is to maintain the security of an organization's IT systems.**

○ Yes

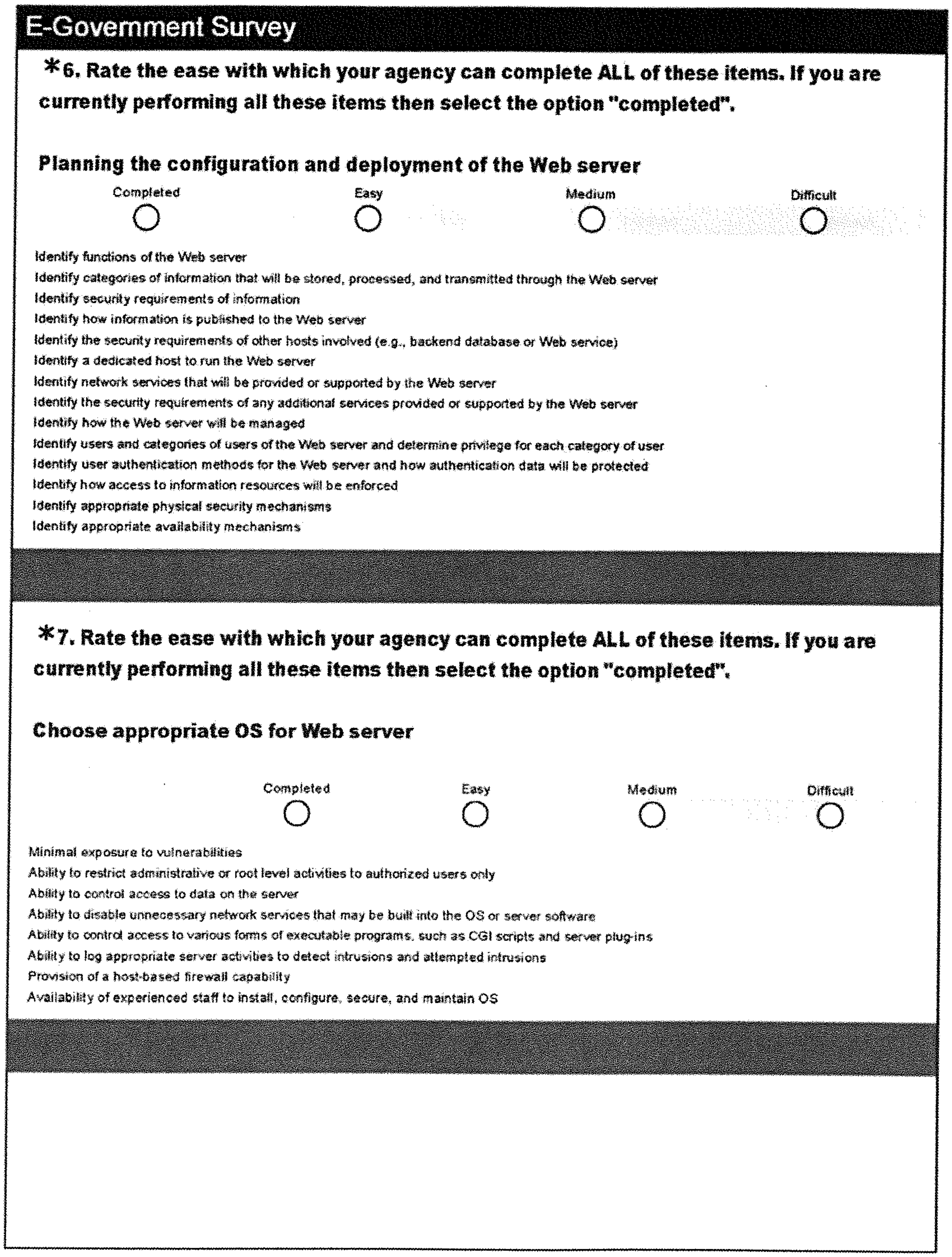
○ No

***5. What is the total IT budget (salaries, expenditures, maintenance, etc.) for the current fiscal year ending June 30, 2012?**

Start of E-Government Survey

Thank you for participating in this survey. Your input forms a valuable contribution to this dissertation research project. You will be presented with 32 questions that ask you to rate the ease in which your agency could perform several e-government security tasks. If your agency is already implementing some of these then you can mark your response as "completed" which indicates that your agency is currently performing those said actions.

Please rate these items as honestly as possible. The results of this survey will only be presented in aggregate format.



E-Government Survey

***6. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Planning the configuration and deployment of the Web server

Completed	Easy	Medium	Difficult
○	○	○	○

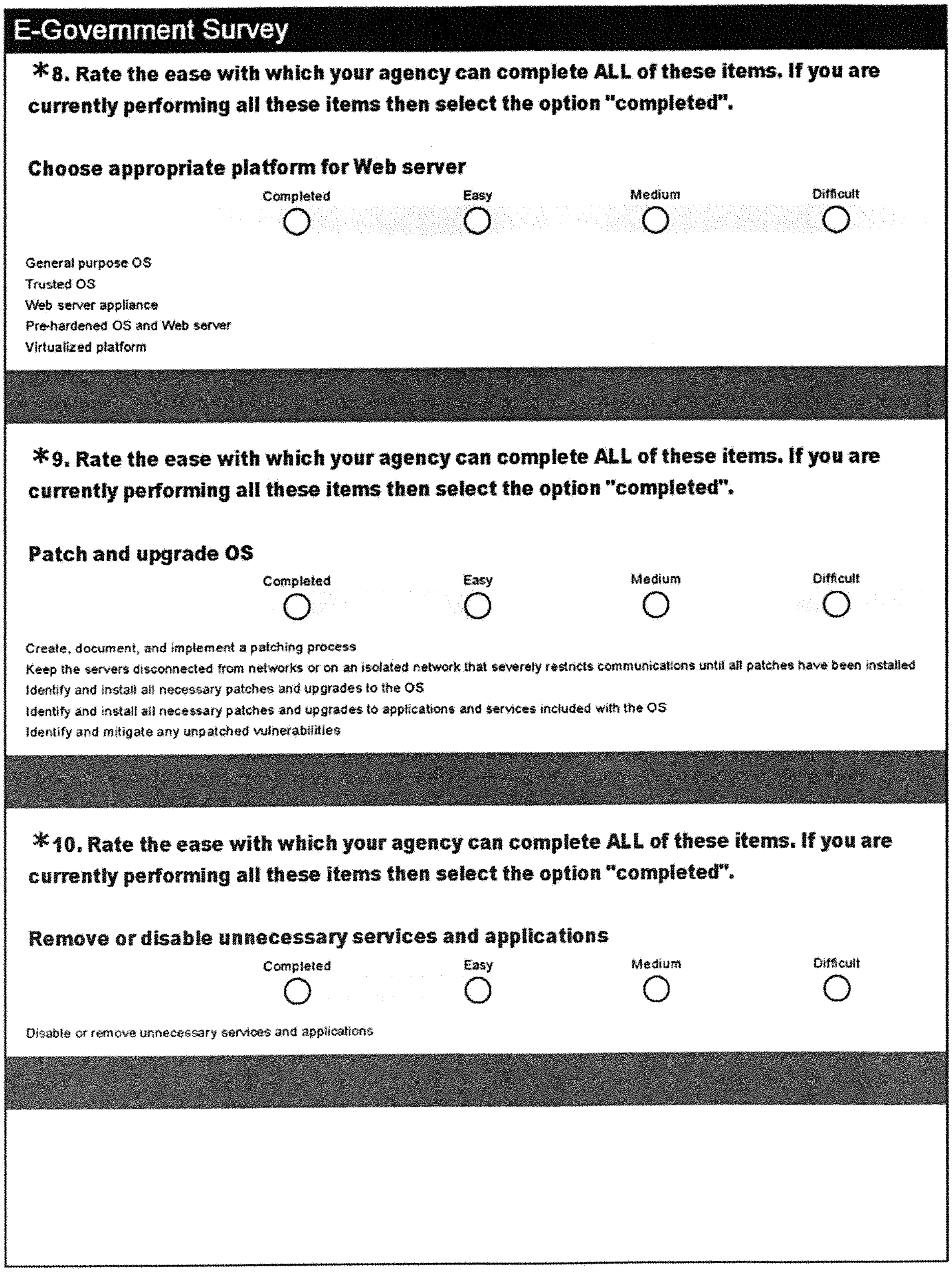
Identify functions of the Web server
Identify categories of information that will be stored, processed, and transmitted through the Web server
Identify security requirements of information
Identify how information is published to the Web server
Identify the security requirements of other hosts involved (e.g., backend database or Web service)
Identify a dedicated host to run the Web server
Identify network services that will be provided or supported by the Web server
Identify the security requirements of any additional services provided or supported by the Web server
Identify how the Web server will be managed
Identify users and categories of users of the Web server and determine privilege for each category of user
Identify user authentication methods for the Web server and how authentication data will be protected
Identify how access to information resources will be enforced
Identify appropriate physical security mechanisms
Identify appropriate availability mechanisms

***7. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Choose appropriate OS for Web server

Completed	Easy	Medium	Difficult
○	○	○	○

Minimal exposure to vulnerabilities
Ability to restrict administrative or root level activities to authorized users only
Ability to control access to data on the server
Ability to disable unnecessary network services that may be built into the OS or server software
Ability to control access to various forms of executable programs, such as CGI scripts and server plug-ins
Ability to log appropriate server activities to detect intrusions and attempted intrusions
Provision of a host-based firewall capability
Availability of experienced staff to install, configure, secure, and maintain OS



E-Government Survey

***8. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Choose appropriate platform for Web server

Completed	Easy	Medium	Difficult
○	○	○	○

General purpose OS
Trusted OS
Web server appliance
Pre-hardened OS and Web server
Virtualized platform

***9. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Patch and upgrade OS

Completed	Easy	Medium	Difficult
○	○	○	○

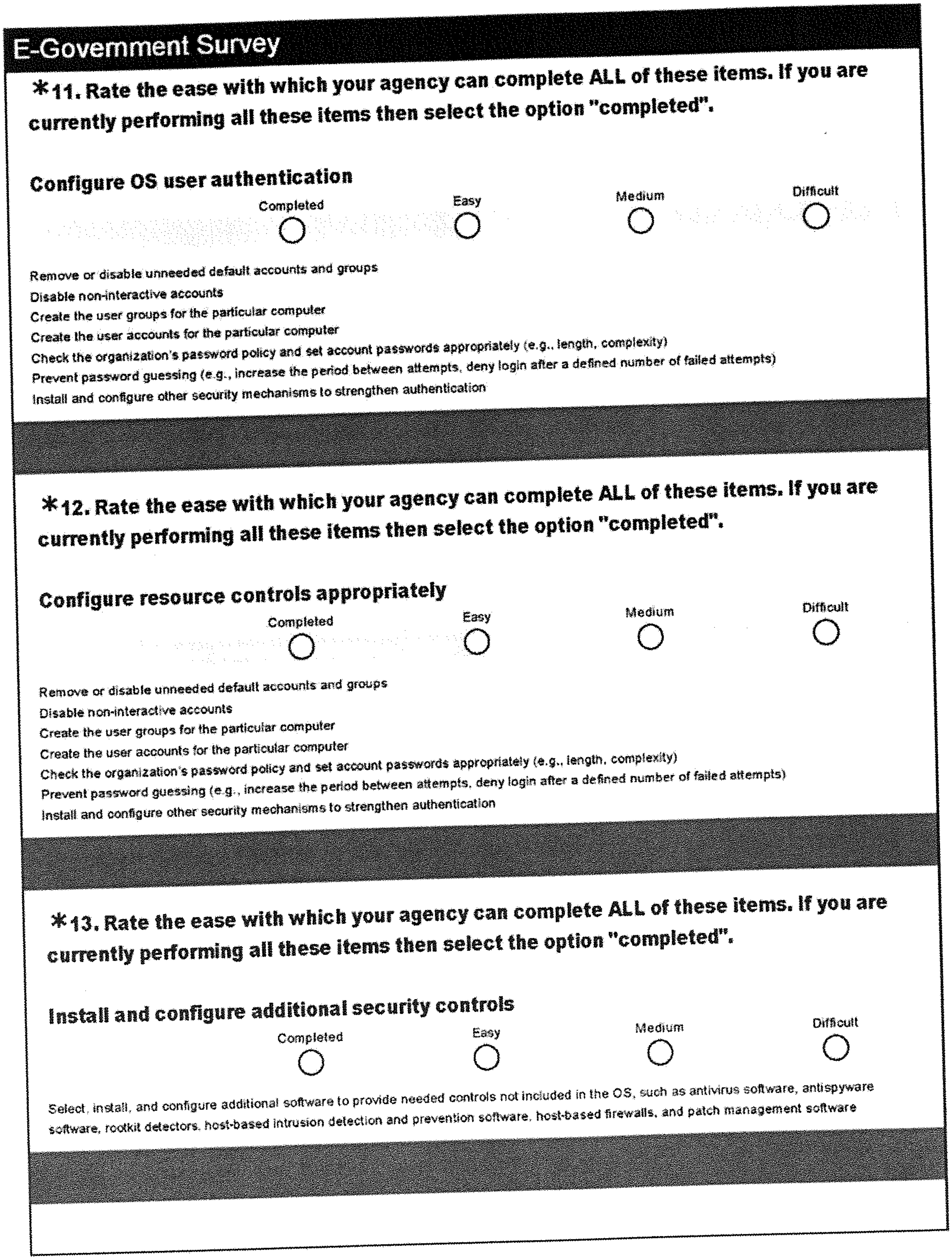
Create, document, and implement a patching process
Keep the servers disconnected from networks or on an isolated network that severely restricts communications until all patches have been installed
Identify and install all necessary patches and upgrades to the OS
Identify and install all necessary patches and upgrades to applications and services included with the OS
Identify and mitigate any unpatched vulnerabilities

***10. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Remove or disable unnecessary services and applications

Completed	Easy	Medium	Difficult
○	○	○	○

Disable or remove unnecessary services and applications



E-Government Survey

*11. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Configure OS user authentication

Completed	Easy	Medium	Difficult
○	○	○	○

Remove or disable unneeded default accounts and groups
Disable non-interactive accounts
Create the user groups for the particular computer
Create the user accounts for the particular computer
Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)
Prevent password guessing (e.g., increase the period between attempts, deny login after a defined number of failed attempts)
Install and configure other security mechanisms to strengthen authentication

*12. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Configure resource controls appropriately

Completed	Easy	Medium	Difficult
○	○	○	○

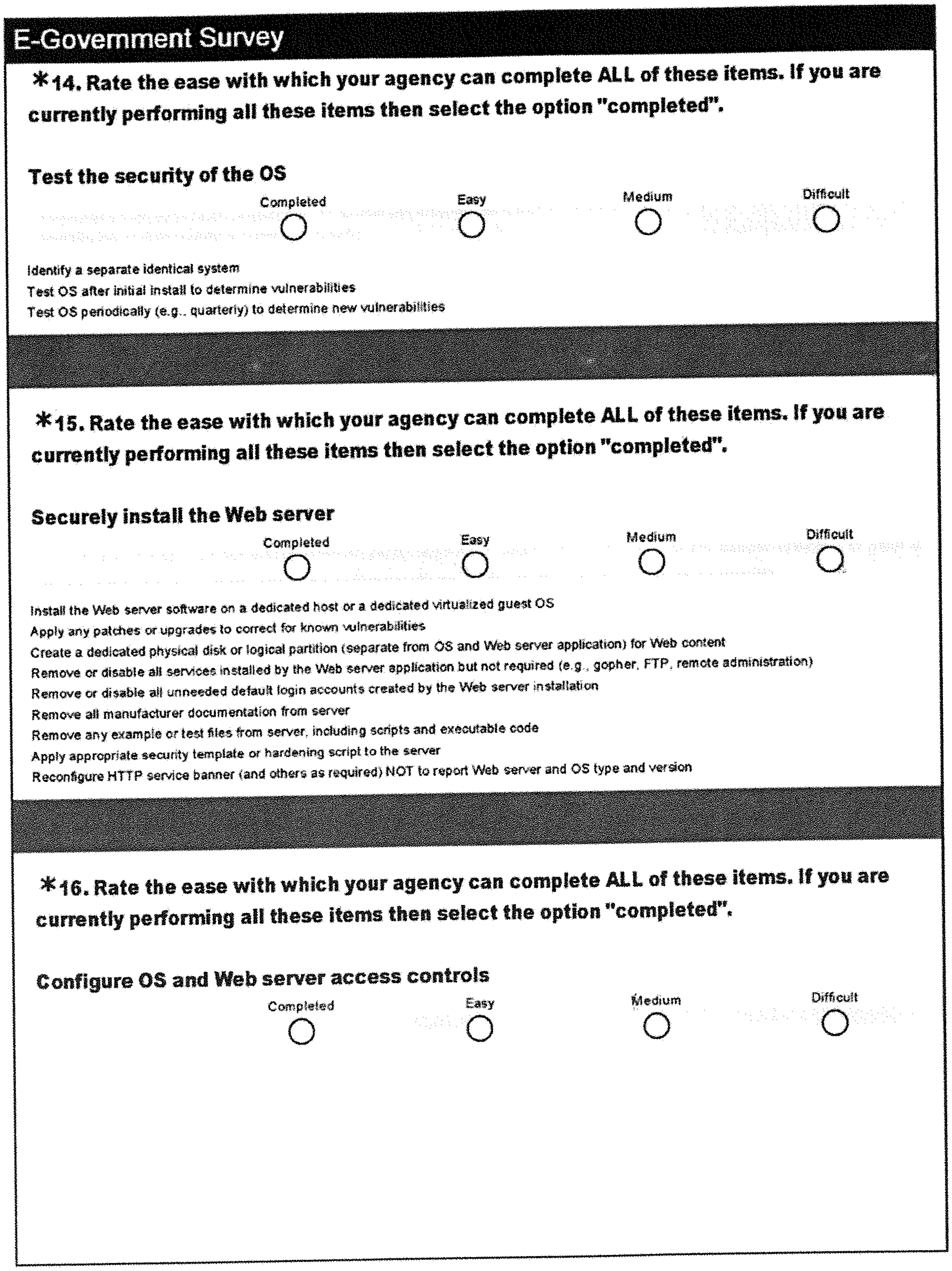
Remove or disable unneeded default accounts and groups
Disable non-interactive accounts
Create the user groups for the particular computer
Create the user accounts for the particular computer
Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)
Prevent password guessing (e.g., increase the period between attempts, deny login after a defined number of failed attempts)
Install and configure other security mechanisms to strengthen authentication

*13. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Install and configure additional security controls

Completed	Easy	Medium	Difficult
○	○	○	○

Select, install, and configure additional software to provide needed controls not included in the OS, such as antivirus software, antispyware software, rootkit detectors, host-based intrusion detection and prevention software, host-based firewalls, and patch management software



E-Government Survey

***14. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Test the security of the OS

Completed	Easy	Medium	Difficult
○	○	○	○

Identify a separate identical system
Test OS after initial install to determine vulnerabilities
Test OS periodically (e.g., quarterly) to determine new vulnerabilities

***15. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Securely install the Web server

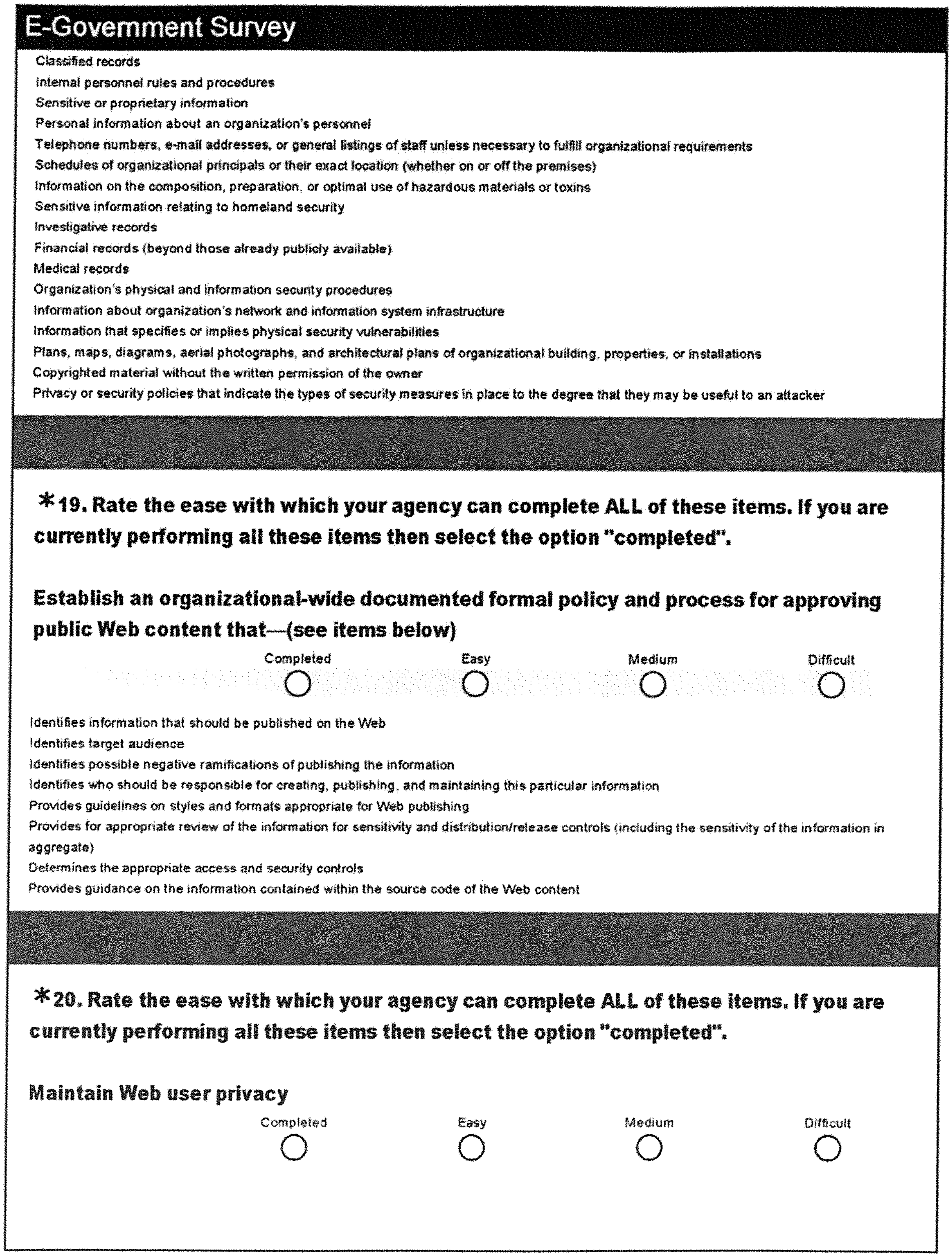
Completed	Easy	Medium	Difficult
○	○	○	○

Install the Web server software on a dedicated host or a dedicated virtualized guest OS
Apply any patches or upgrades to correct for known vulnerabilities
Create a dedicated physical disk or logical partition (separate from OS and Web server application) for Web content
Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, remote administration)
Remove or disable all unneeded default login accounts created by the Web server installation
Remove all manufacturer documentation from server
Remove any example or test files from server, including scripts and executable code
Apply appropriate security template or hardening script to the server
Reconfigure HTTP service banner (and others as required) NOT to report Web server and OS type and version

***16. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Configure OS and Web server access controls

Completed	Easy	Medium	Difficult
○	○	○	○



E-Government Survey

Classified records
Internal personnel rules and procedures
Sensitive or proprietary information
Personal information about an organization's personnel
Telephone numbers, e-mail addresses, or general listings of staff unless necessary to fulfill organizational requirements
Schedules of organizational principals or their exact location (whether on or off the premises)
Information on the composition, preparation, or optimal use of hazardous materials or toxins
Sensitive information relating to homeland security
Investigative records
Financial records (beyond those already publicly available)
Medical records
Organization's physical and information security procedures
Information about organization's network and information system infrastructure
Information that specifies or implies physical security vulnerabilities
Plans, maps, diagrams, aerial photographs, and architectural plans of organizational building, properties, or installations
Copyrighted material without the written permission of the owner
Privacy or security policies that indicate the types of security measures in place to the degree that they may be useful to an attacker

***19. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Establish an organizational-wide documented formal policy and process for approving public Web content that—(see items below)

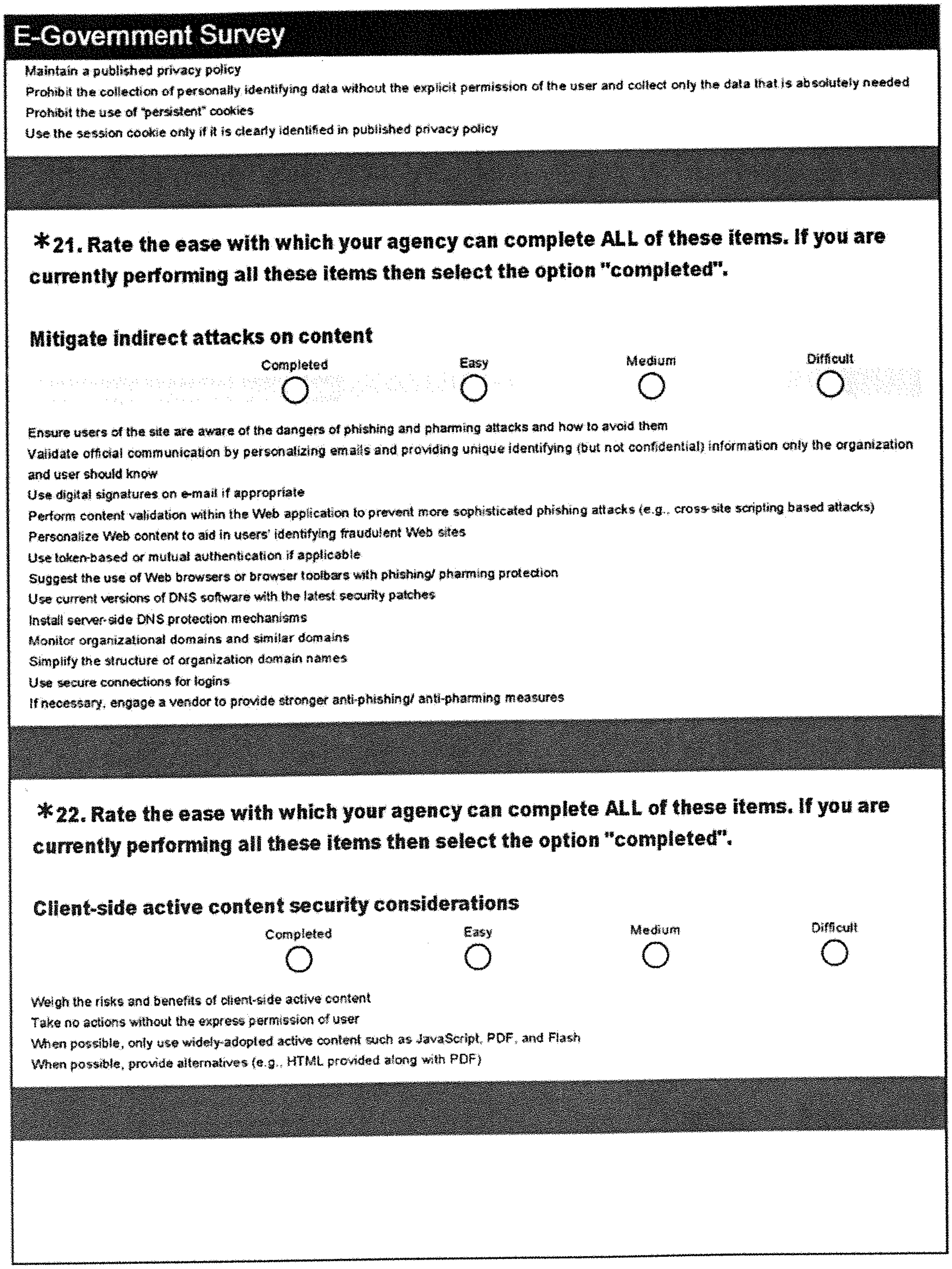
Completed	Easy	Medium	Difficult
○	○	○	○

Identifies information that should be published on the Web
Identifies target audience
Identifies possible negative ramifications of publishing the information
Identifies who should be responsible for creating, publishing, and maintaining this particular information
Provides guidelines on styles and formats appropriate for Web publishing
Provides for appropriate review of the information for sensitivity and distribution/release controls (including the sensitivity of the information in aggregate)
Determines the appropriate access and security controls
Provides guidance on the information contained within the source code of the Web content

***20. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Maintain Web user privacy

Completed	Easy	Medium	Difficult
○	○	○	○



E-Government Survey

Maintain a published privacy policy
Prohibit the collection of personally identifying data without the explicit permission of the user and collect only the data that is absolutely needed
Prohibit the use of "persistent" cookies
Use the session cookie only if it is clearly identified in published privacy policy

***21. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Mitigate indirect attacks on content

Completed	Easy	Medium	Difficult
○	○	○	○

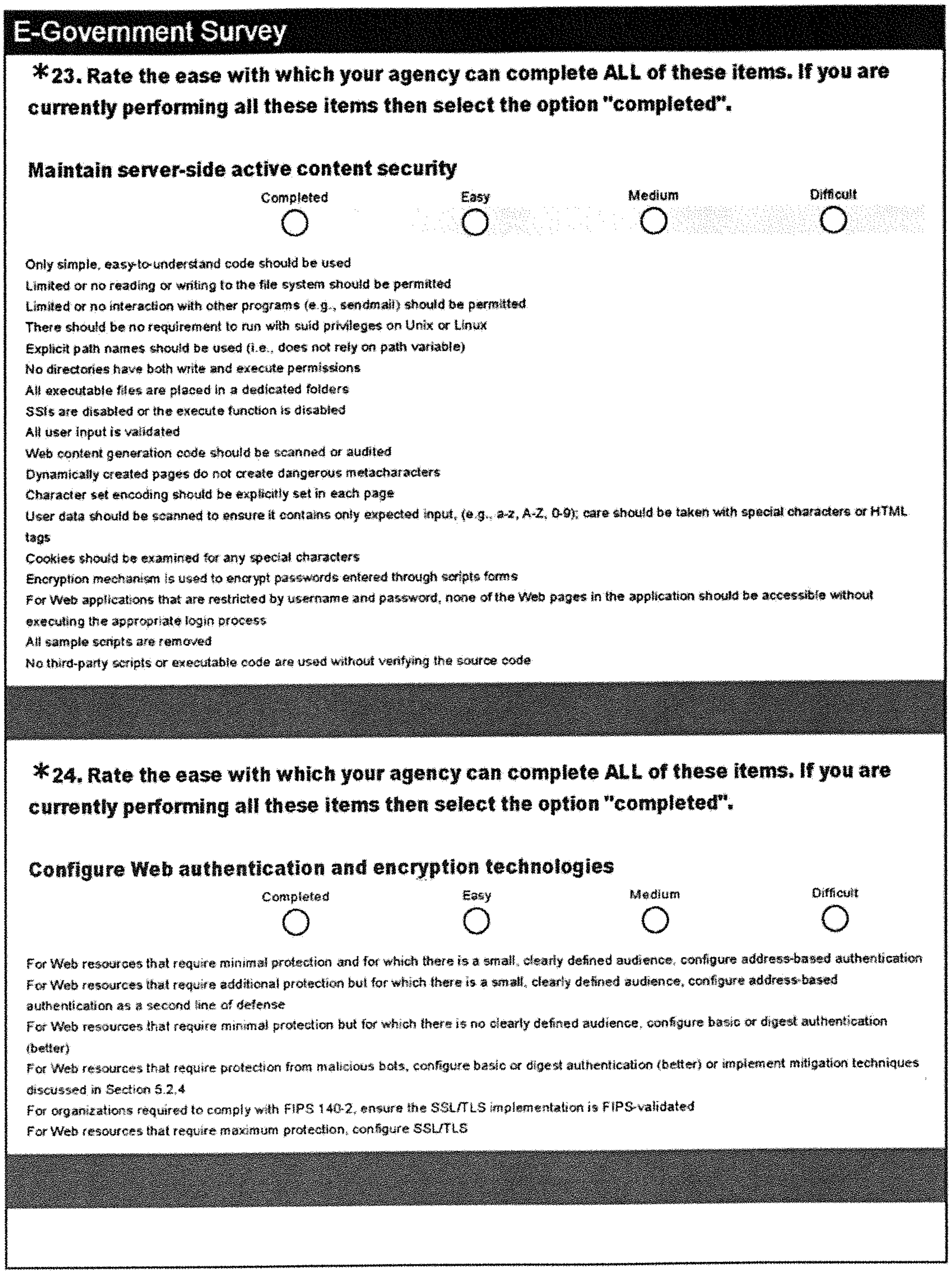
Ensure users of the site are aware of the dangers of phishing and pharming attacks and how to avoid them
Validate official communication by personalizing emails and providing unique identifying (but not confidential) information only the organization and user should know
Use digital signatures on e-mail if appropriate
Perform content validation within the Web application to prevent more sophisticated phishing attacks (e.g., cross-site scripting based attacks)
Personalize Web content to aid in users' identifying fraudulent Web sites
Use token-based or mutual authentication if applicable
Suggest the use of Web browsers or browser toolbars with phishing/ pharming protection
Use current versions of DNS software with the latest security patches
Install server-side DNS protection mechanisms
Monitor organizational domains and similar domains
Simplify the structure of organization domain names
Use secure connections for logins
If necessary, engage a vendor to provide stronger anti-phishing/ anti-pharming measures

***22. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Client-side active content security considerations

Completed	Easy	Medium	Difficult
○	○	○	○

Weigh the risks and benefits of client-side active content
Take no actions without the express permission of user
When possible, only use widely-adopted active content such as JavaScript, PDF, and Flash
When possible, provide alternatives (e.g., HTML provided along with PDF)



E-Government Survey

*23. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Maintain server-side active content security

	Completed	Easy	Medium	Difficult
	○	○	○	○

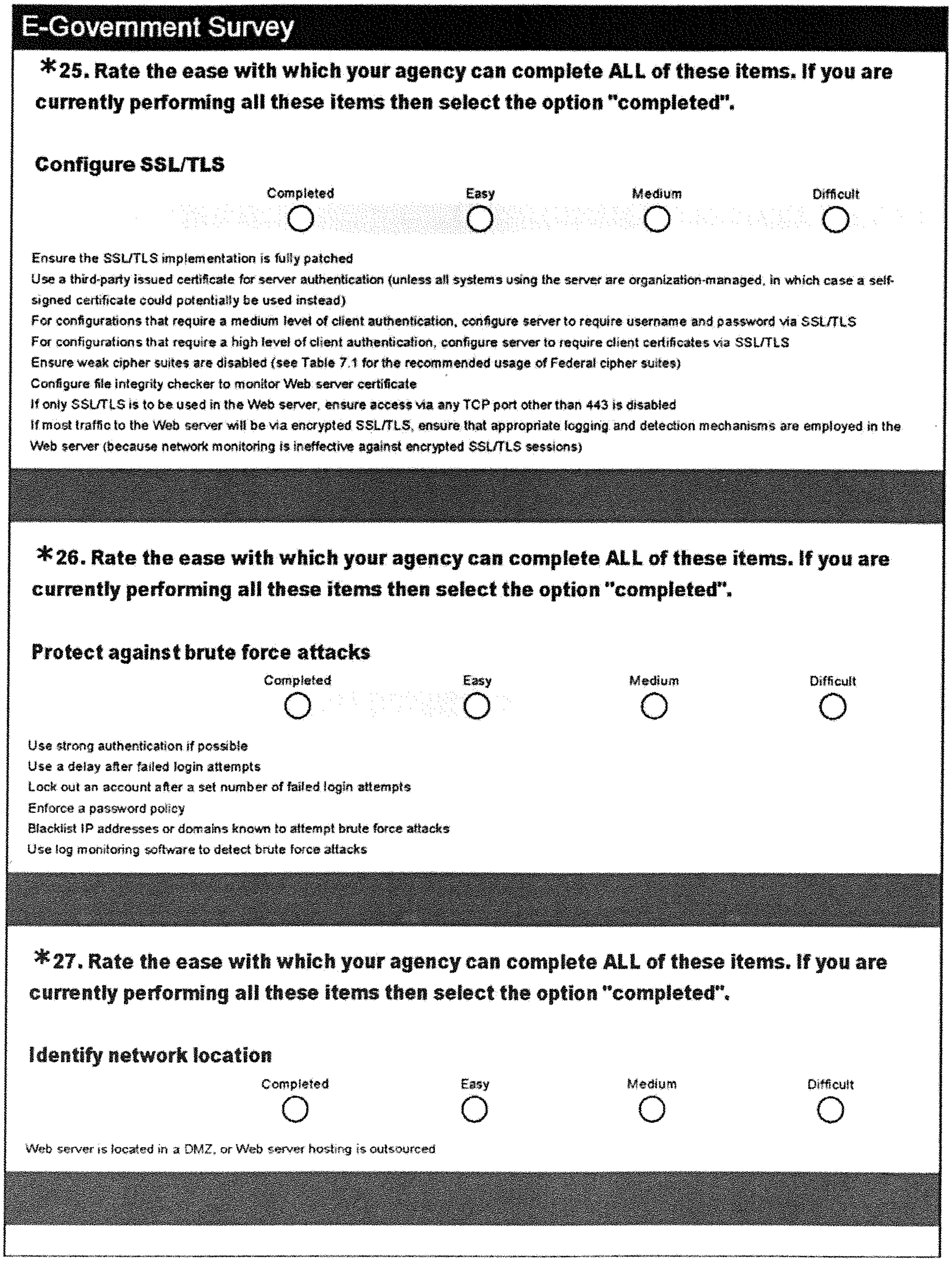
Only simple, easy-to-understand code should be used
Limited or no reading or writing to the file system should be permitted
Limited or no interaction with other programs (e.g., sendmail) should be permitted
There should be no requirement to run with suid privileges on Unix or Linux
Explicit path names should be used (i.e., does not rely on path variable)
No directories have both write and execute permissions
All executable files are placed in a dedicated folders
SSIs are disabled or the execute function is disabled
All user input is validated
Web content generation code should be scanned or audited
Dynamically created pages do not create dangerous metacharacters
Character set encoding should be explicitly set in each page
User data should be scanned to ensure it contains only expected input, (e.g., a-z, A-Z, 0-9); care should be taken with special characters or HTML tags
Cookies should be examined for any special characters
Encryption mechanism is used to encrypt passwords entered through scripts forms
For Web applications that are restricted by username and password, none of the Web pages in the application should be accessible without executing the appropriate login process
All sample scripts are removed
No third-party scripts or executable code are used without verifying the source code

*24. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Configure Web authentication and encryption technologies

	Completed	Easy	Medium	Difficult
	○	○	○	○

For Web resources that require minimal protection and for which there is a small, clearly defined audience, configure address-based authentication
For Web resources that require additional protection but for which there is a small, clearly defined audience, configure address-based authentication as a second line of defense
For Web resources that require minimal protection but for which there is no clearly defined audience, configure basic or digest authentication (better)
For Web resources that require protection from malicious bots, configure basic or digest authentication (better) or implement mitigation techniques discussed in Section 5.2.4
For organizations required to comply with FIPS 140-2, ensure the SSL/TLS implementation is FIPS-validated
For Web resources that require maximum protection, configure SSL/TLS



E-Government Survey

*25. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Configure SSL/TLS

Completed	Easy	Medium	Difficult
○	○	○	○

Ensure the SSL/TLS implementation is fully patched
Use a third-party issued certificate for server authentication (unless all systems using the server are organization-managed, in which case a self-signed certificate could potentially be used instead)
For configurations that require a medium level of client authentication, configure server to require username and password via SSL/TLS
For configurations that require a high level of client authentication, configure server to require client certificates via SSL/TLS
Ensure weak cipher suites are disabled (see Table 7.1 for the recommended usage of Federal cipher suites)
Configure file integrity checker to monitor Web server certificate
If only SSL/TLS is to be used in the Web server, ensure access via any TCP port other than 443 is disabled
If most traffic to the Web server will be via encrypted SSL/TLS, ensure that appropriate logging and detection mechanisms are employed in the Web server (because network monitoring is ineffective against encrypted SSL/TLS sessions)

*26. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Protect against brute force attacks

Completed	Easy	Medium	Difficult
○	○	○	○

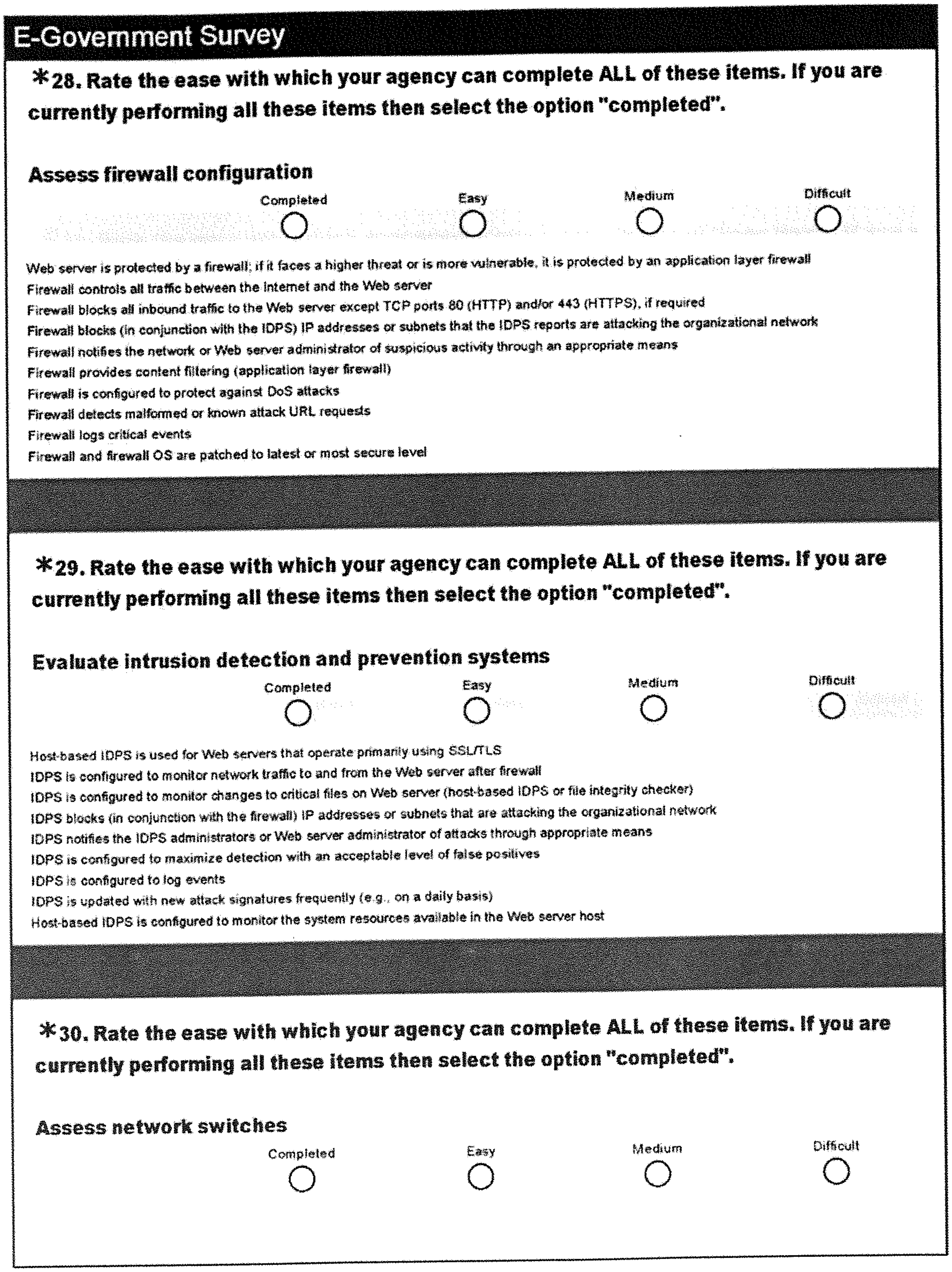
Use strong authentication if possible
Use a delay after failed login attempts
Lock out an account after a set number of failed login attempts
Enforce a password policy
Blacklist IP addresses or domains known to attempt brute force attacks
Use log monitoring software to detect brute force attacks

*27. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".

Identify network location

Completed	Easy	Medium	Difficult
○	○	○	○

Web server is located in a DMZ, or Web server hosting is outsourced



E-Government Survey

***28. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Assess firewall configuration

Completed	Easy	Medium	Difficult
○	○	○	○

Web server is protected by a firewall; if it faces a higher threat or is more vulnerable, it is protected by an application layer firewall
Firewall controls all traffic between the Internet and the Web server
Firewall blocks all inbound traffic to the Web server except TCP ports 80 (HTTP) and/or 443 (HTTPS), if required
Firewall blocks (in conjunction with the IDPS) IP addresses or subnets that the IDPS reports are attacking the organizational network
Firewall notifies the network or Web server administrator of suspicious activity through an appropriate means
Firewall provides content filtering (application layer firewall)
Firewall is configured to protect against DoS attacks
Firewall detects malformed or known attack URL requests
Firewall logs critical events
Firewall and firewall OS are patched to latest or most secure level

***29. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Evaluate intrusion detection and prevention systems

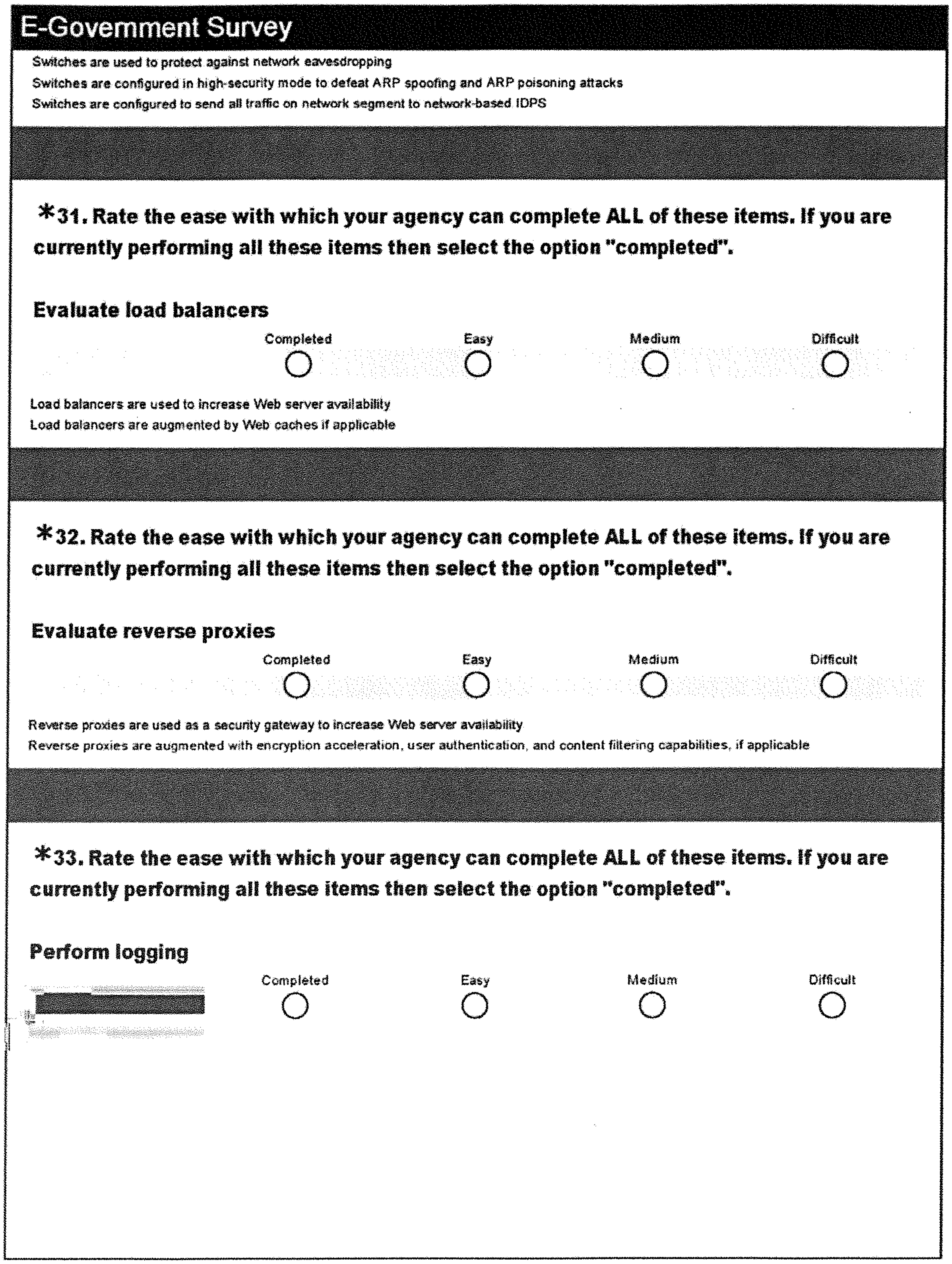
Completed	Easy	Medium	Difficult
○	○	○	○

Host-based IDPS is used for Web servers that operate primarily using SSL/TLS
IDPS is configured to monitor network traffic to and from the Web server after firewall
IDPS is configured to monitor changes to critical files on Web server (host-based IDPS or file integrity checker)
IDPS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
IDPS notifies the IDPS administrators or Web server administrator of attacks through appropriate means
IDPS is configured to maximize detection with an acceptable level of false positives
IDPS is configured to log events
IDPS is updated with new attack signatures frequently (e.g., on a daily basis)
Host-based IDPS is configured to monitor the system resources available in the Web server host

***30. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Assess network switches

Completed	Easy	Medium	Difficult
○	○	○	○



E-Government Survey

Switches are used to protect against network eavesdropping

Switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks

Switches are configured to send all traffic on network segment to network-based IDPS

***31. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Evaluate load balancers

Completed	Easy	Medium	Difficult
○	○	○	○

Load balancers are used to increase Web server availability

Load balancers are augmented by Web caches if applicable

***32. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Evaluate reverse proxies

Completed	Easy	Medium	Difficult
○	○	○	○

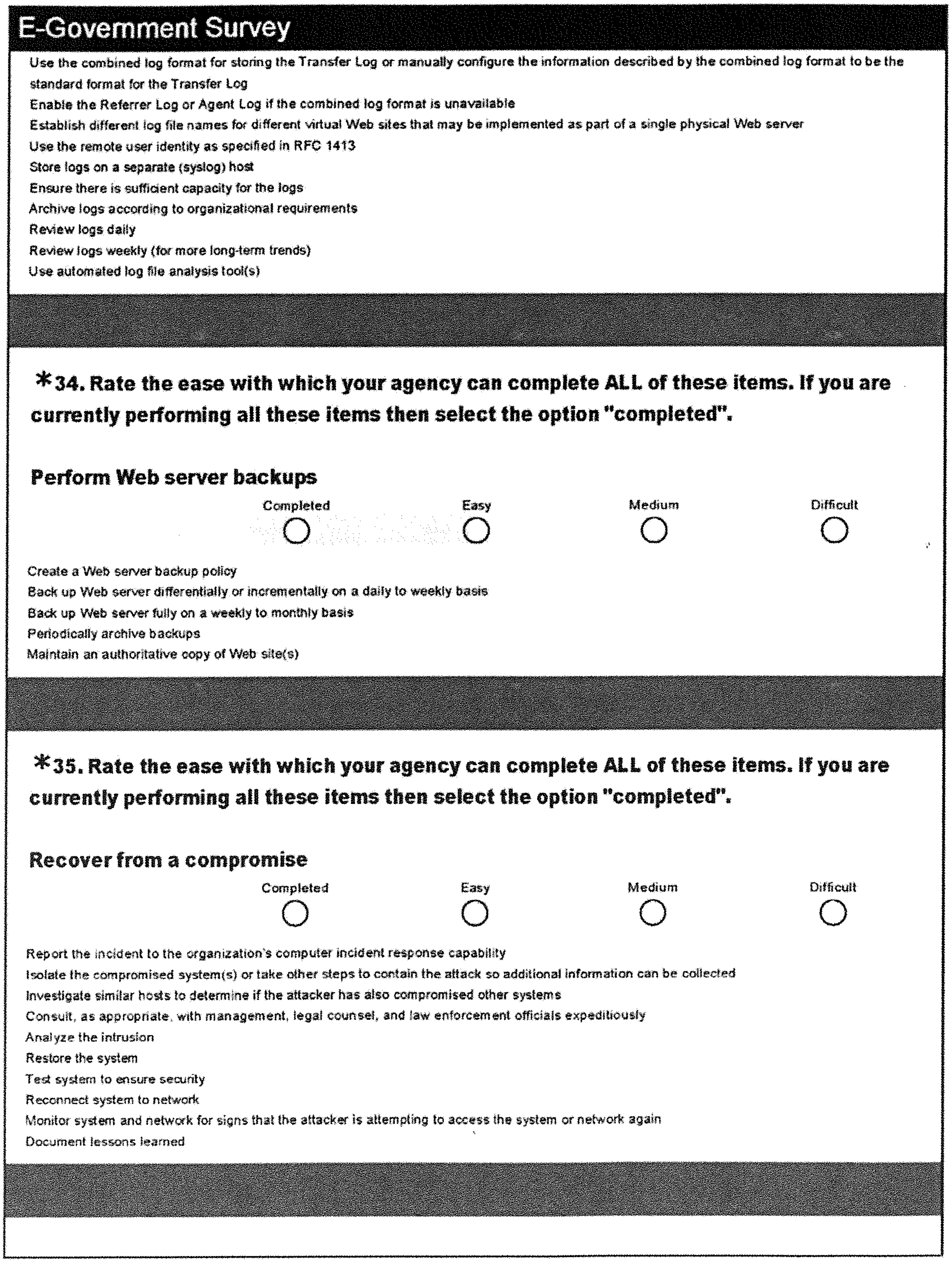
Reverse proxies are used as a security gateway to increase Web server availability

Reverse proxies are augmented with encryption acceleration, user authentication, and content filtering capabilities, if applicable

***33. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Perform logging

Completed	Easy	Medium	Difficult
○	○	○	○



E-Government Survey

Use the combined log format for storing the Transfer Log or manually configure the information described by the combined log format to be the standard format for the Transfer Log
Enable the Referrer Log or Agent Log if the combined log format is unavailable
Establish different log file names for different virtual Web sites that may be implemented as part of a single physical Web server
Use the remote user identity as specified in RFC 1413
Store logs on a separate (syslog) host
Ensure there is sufficient capacity for the logs
Archive logs according to organizational requirements
Review logs daily
Review logs weekly (for more long-term trends)
Use automated log file analysis tool(s)

***34. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Perform Web server backups

Completed	Easy	Medium	Difficult
○	○	○	○

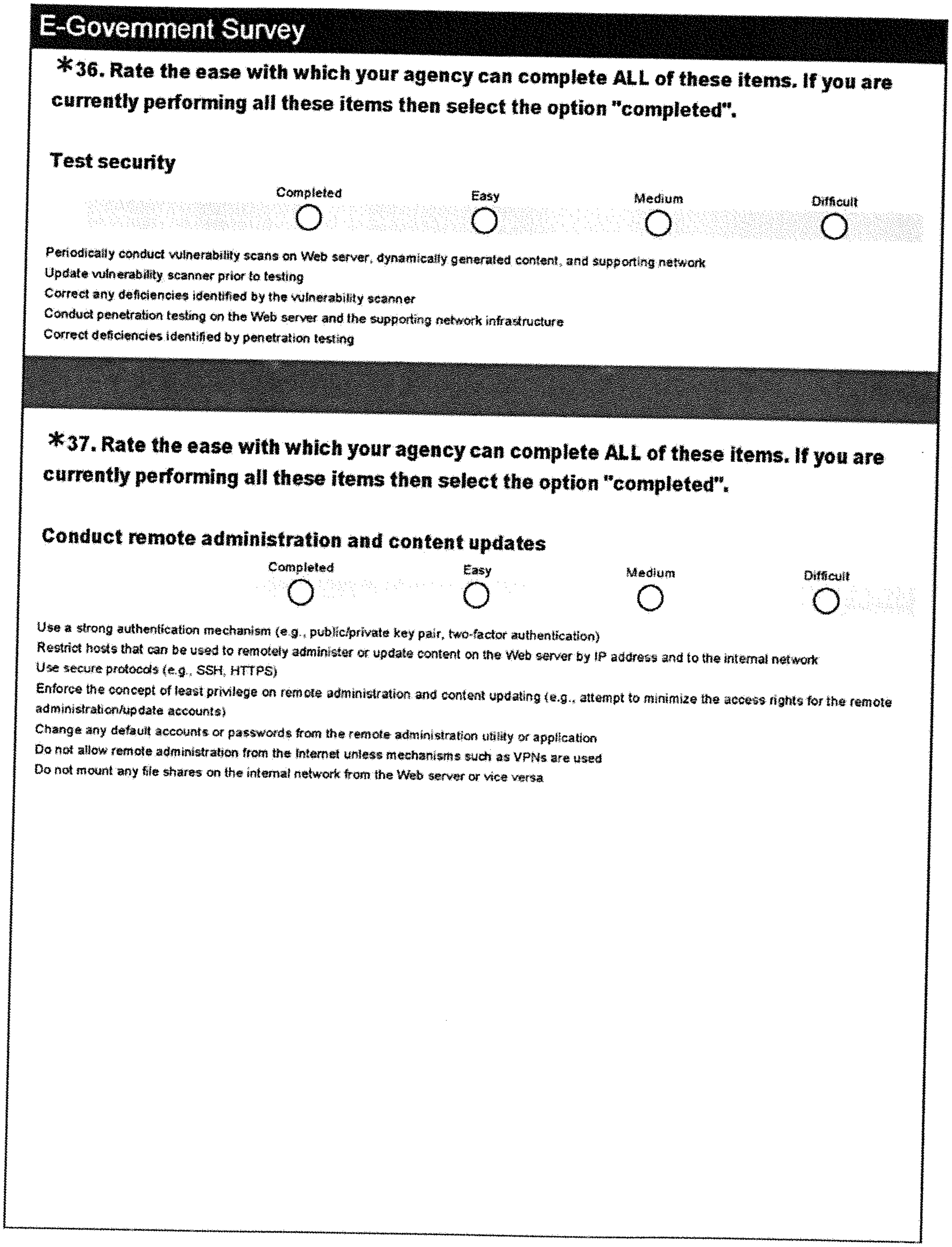
Create a Web server backup policy
Back up Web server differentially or incrementally on a daily to weekly basis
Back up Web server fully on a weekly to monthly basis
Periodically archive backups
Maintain an authoritative copy of Web site(s)

***35. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Recover from a compromise

Completed	Easy	Medium	Difficult
○	○	○	○

Report the incident to the organization's computer incident response capability
Isolate the compromised system(s) or take other steps to contain the attack so additional information can be collected
Investigate similar hosts to determine if the attacker has also compromised other systems
Consult, as appropriate, with management, legal counsel, and law enforcement officials expeditiously
Analyze the intrusion
Restore the system
Test system to ensure security
Reconnect system to network
Monitor system and network for signs that the attacker is attempting to access the system or network again
Document lessons learned



E-Government Survey

***36. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Test security

Completed	Easy	Medium	Difficult
○	○	○	○

Periodically conduct vulnerability scans on Web server, dynamically generated content, and supporting network
Update vulnerability scanner prior to testing
Correct any deficiencies identified by the vulnerability scanner
Conduct penetration testing on the Web server and the supporting network infrastructure
Correct deficiencies identified by penetration testing

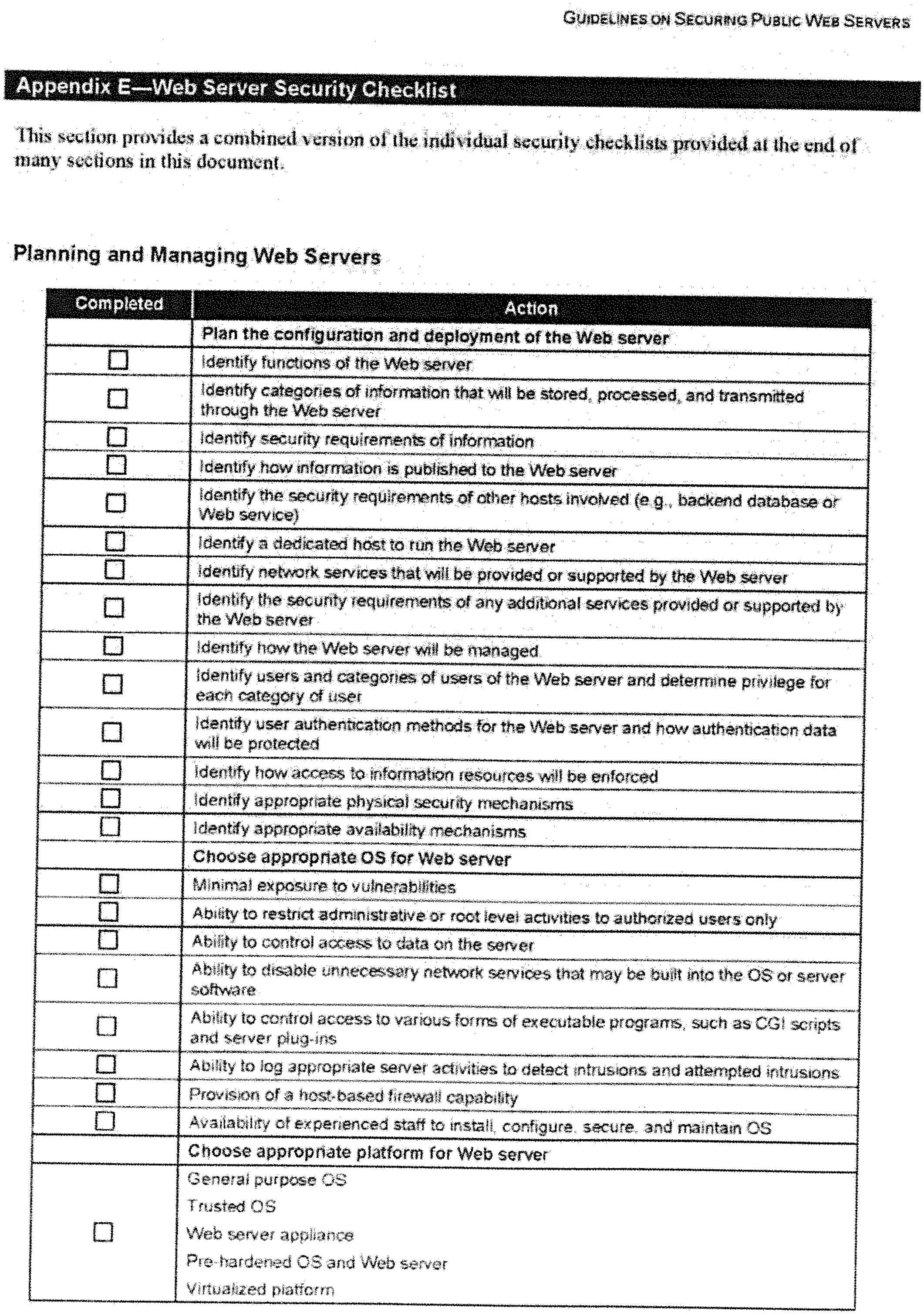
***37. Rate the ease with which your agency can complete ALL of these items. If you are currently performing all these items then select the option "completed".**

Conduct remote administration and content updates

Completed	Easy	Medium	Difficult
○	○	○	○

Use a strong authentication mechanism (e.g., public/private key pair, two-factor authentication)
Restrict hosts that can be used to remotely administer or update content on the Web server by IP address and to the internal network
Use secure protocols (e.g., SSH, HTTPS)
Enforce the concept of least privilege on remote administration and content updating (e.g., attempt to minimize the access rights for the remote administration/update accounts)
Change any default accounts or passwords from the remote administration utility or application
Do not allow remote administration from the Internet unless mechanisms such as VPNs are used
Do not mount any file shares on the internal network from the Web server or vice versa

APPENDIX B: NIST SP800-44 SECURITY CHECKLISTS



Appendix E—Web Server Security Checklist

This section provides a combined version of the individual security checklists provided at the end of many sections in this document.

Planning and Managing Web Servers

Completed	Action
	Plan the configuration and deployment of the Web server
□	Identify functions of the Web server
□	Identify categories of information that will be stored, processed, and transmitted through the Web server
□	Identify security requirements of information
□	Identify how information is published to the Web server
□	Identify the security requirements of other hosts involved (e.g., backend database or Web service)
□	Identify a dedicated host to run the Web server
□	Identify network services that will be provided or supported by the Web server
□	Identify the security requirements of any additional services provided or supported by the Web server
□	Identify how the Web server will be managed
□	Identify users and categories of users of the Web server and determine privilege for each category of user
□	Identify user authentication methods for the Web server and how authentication data will be protected
□	Identify how access to information resources will be enforced
□	Identify appropriate physical security mechanisms
□	Identify appropriate availability mechanisms
	Choose appropriate OS for Web server
□	Minimal exposure to vulnerabilities
□	Ability to restrict administrative or root level activities to authorized users only
□	Ability to control access to data on the server
□	Ability to disable unnecessary network services that may be built into the OS or server software
□	Ability to control access to various forms of executable programs, such as CGI scripts and server plug-ins
□	Ability to log appropriate server activities to detect intrusions and attempted intrusions
□	Provision of a host-based firewall capability
□	Availability of experienced staff to install, configure, secure, and maintain OS
	Choose appropriate platform for Web server
□	General purpose OS Trusted OS Web server appliance Pre-hardened OS and Web server Virtualized platform

Securing the Web Server Operating System

Completed	Action
	Patch and upgrade OS
□	Create, document, and implement a patching process
□	Keep the servers disconnected from networks or on an isolated network that severely restricts communications until all patches have been installed
□	Identify and install all necessary patches and upgrades to the OS
□	Identify and install all necessary patches and upgrades to applications and services included with the OS
□	Identify and mitigate any unpatched vulnerabilities
	Remove or disable unnecessary services and applications
□	Disable or remove unnecessary services and applications
	Configure OS user authentication
□	Remove or disable unneeded default accounts and groups
□	Disable non-interactive accounts
□	Create the user groups for the particular computer
□	Create the user accounts for the particular computer
□	Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)
□	Prevent password guessing (e.g., increase the period between attempts, deny login after a defined number of failed attempts)
□	Install and configure other security mechanisms to strengthen authentication
	Configure resource controls appropriately
□	Deny read access to unnecessary files and directories
□	Deny write access to unnecessary files and directories
□	Limit the execution privilege of system tools to system administrators
	Install and configure additional security controls
□	Select, install, and configure additional software to provide needed controls not included in the OS, such as antivirus software, antispyware software, rootkit detectors, host-based intrusion detection and prevention software, host-based firewalls, and patch management software
	Test the security of the OS
□	Identify a separate identical system
□	Test OS after initial install to determine vulnerabilities
□	Test OS periodically (e.g., quarterly) to determine new vulnerabilities

Securing the Web Server

Completed	Action
	Securely install the Web server
□	Install the Web server software on a dedicated host or a dedicated virtualized guest OS
□	Apply any patches or upgrades to correct for known vulnerabilities
□	Create a dedicated physical disk or logical partition (separate from OS and Web server application) for Web content

Completed	Action
□	Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, remote administration)
□	Remove or disable all unneeded default login accounts created by the Web server installation
□	Remove all manufacturer documentation from server
□	Remove any example or test files from server, including scripts and executable code
□	Apply appropriate security template or hardening script to the server
□	Reconfigure HTTP service banner (and others as required) NOT to report Web server and OS type and version
	Configure OS and Web server access controls
□	Configure the Web server process to run as a user with a strictly limited set of privileges
□	Configure the Web server so that Web content files can be read but not written by service processes
□	Configure the Web server so that service processes cannot write to the directories where public Web content is stored
□	Configure the Web server so that only processes authorized for Web server administration can write Web content files
□	Configure the host OS so that the Web server can write log files but not read them
□	Configure the host OS so that temporary files created by the Web server application are restricted to a specified and appropriately protected subdirectory
□	Configure the host OS so that access to any temporary files created by the Web server application is limited to the service processes that created the files
□	Install Web content on a different hard drive or logical partition than the OS and Web server application
□	If uploads are allowed to the Web server, configure it so that a limit is placed on the amount of hard drive space that is dedicated for this purpose; uploads should be placed on a separate partition
□	Ensure that log files are stored in a location that is sized appropriately; log files should be placed on a separate partition
□	Configure the maximum number of Web server processes and/or network connections that the Web server should allow
□	Ensure that any virtualized guest OSs follow this checklist
□	Ensure users and administrators are able to change passwords
□	Disable users after a specified period of inactivity
□	Ensure each user and administrator has a unique ID
	Configure a secure Web content directory
□	Dedicate a single hard drive or logical partition for Web content and establish related subdirectories exclusively for Web server content files, including graphics but excluding scripts and other programs
□	Define a single directory exclusively for all external scripts or programs executed as part of Web server content (e.g., CGI, ASP)
□	Disable the execution of scripts that are not exclusively under the control of administrative accounts. This action is accomplished by creating and controlling access to a separate directory intended to contain authorized scripts
□	Disable the use of hard or symbolic links (e.g., shortcuts for Windows)

Completed	Action
□	Define a complete Web content access matrix. Identify which folders and files within the Web server document should be restricted and which should be accessible (and by whom)
□	Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)
□	Use the robots.txt file, if appropriate
□	Configure anti-spambot protection, if appropriate (e.g., CAPTCHAs, nofollow, or keyword filtering)

Securing Web Content

Completed	Action
	Ensure that none of the following types of information are available on or through a public Web server
□	Classified records
□	Internal personnel rules and procedures
□	Sensitive or proprietary information
□	Personal information about an organization's personnel
□	Telephone numbers, e-mail addresses, or general listings of staff unless necessary to fulfill organizational requirements
□	Schedules of organizational principals or their exact location (whether on or off the premises)
□	Information on the composition, preparation, or optimal use of hazardous materials or toxins
□	Sensitive information relating to homeland security
□	Investigative records
□	Financial records (beyond those already publicly available)
□	Medical records
□	Organization's physical and information security procedures
□	Information about organization's network and information system infrastructure
□	Information that specifies or implies physical security vulnerabilities
□	Plans, maps, diagrams, aerial photographs, and architectural plans of organizational building, properties, or installations
□	Copyrighted material without the written permission of the owner
□	Privacy or security policies that indicate the types of security measures in place to the degree that they may be useful to an attacker
	Establish an organizational-wide documented formal policy and process for approving public Web content that—
□	Identifies information that should be published on the Web
□	Identifies target audience
□	Identifies possible negative ramifications of publishing the information
□	Identifies who should be responsible for creating, publishing, and maintaining this particular information
□	Provides guidelines on styles and formats appropriate for Web publishing
□	Provides for appropriate review of the information for sensitivity and distribution/release controls (including the sensitivity of the information in aggregate)

Completed	Action
□	Determines the appropriate access and security controls
□	Provides guidance on the information contained within the source code of the Web content
	Maintain Web user privacy
□	Maintain a published privacy policy
□	Prohibit the collection of personally identifying data without the explicit permission of the user and collect only the data that is absolutely needed
□	Prohibit the use of "persistent" cookies
□	Use the session cookie only if it is clearly identified in published privacy policy
	Mitigate indirect attacks on content
□	Ensure users of the site are aware of the dangers of phishing and pharming attacks and how to avoid them
□	Validate official communication by personalizing emails and providing unique identifying (but not confidential) information only the organization and user should know
□	Use digital signatures on e-mail if appropriate
□	Perform content validation within the Web application to prevent more sophisticated phishing attacks (e.g., cross-site scripting based attacks)
□	Personalize Web content to aid in users' identifying fraudulent Web sites
□	Use token-based or mutual authentication if applicable
□	Suggest the use of Web browsers or browser toolbars with phishing/ pharming protection
□	Use current versions of DNS software with the latest security patches
□	Install server-side DNS protection mechanisms
□	Monitor organizational domains and similar domains
□	Simplify the structure of organization domain names
□	Use secure connections for logins
□	If necessary, engage a vendor to provide stronger anti-phishing/ anti-pharming measures
	Client-side active content security considerations
□	Weigh the risks and benefits of client-side active content
□	Take no actions without the express permission of user
□	When possible, only use widely-adopted active content such as JavaScript, PDF, and Flash
□	When possible, provide alternatives (e.g., HTML provided along with PDF)
	Maintain server-side active content security
□	Only simple, easy-to-understand code should be used
□	Limited or no reading or writing to the file system should be permitted
□	Limited or no interaction with other programs (e.g., sendmail) should be permitted
□	There should be no requirement to run with suid privileges on Unix or Linux
□	Explicit path names should be used (i.e., does not rely on path variable)
□	No directories have both write and execute permissions
□	All executable files are placed in a dedicated folders
□	SSIs are disabled or the execute function is disabled
□	All user input is validated

Completed	Action
□	Web content generation code should be scanned or audited
□	Dynamically created pages do not create dangerous metacharacters
□	Character set encoding should be explicitly set in each page
□	User data should be scanned to ensure it contains only expected input, (e.g., a-z, A-Z, 0-9); care should be taken with special characters or HTML tags
□	Cookies should be examined for any special characters
□	Encryption mechanism is used to encrypt passwords entered through scripts forms
□	For Web applications that are restricted by username and password, none of the Web pages in the application should be accessible without executing the appropriate login process
□	All sample scripts are removed
□	No third-party scripts or executable code are used without verifying the source code

Using Authentication and Encryption Technologies for Web Servers

Completed	Action
	Configure Web authentication and encryption technologies
□	For Web resources that require minimal protection and for which there is a small, clearly defined audience, configure address-based authentication
□	For Web resources that require additional protection but for which there is a small, clearly defined audience, configure address-based authentication as a second line of defense
□	For Web resources that require minimal protection but for which there is no clearly defined audience, configure basic or digest authentication (better)
□	For Web resources that require protection from malicious bots, configure basic or digest authentication (better) or implement mitigation techniques discussed in Section 5.2.4
□	For organizations required to comply with FIPS 140-2, ensure the SSL/TLS implementation is FIPS-validated
□	For Web resources that require maximum protection, configure SSL/TLS
	Configure SSL/TLS
□	Ensure the SSL/TLS implementation is fully patched
□	Use a third-party issued certificate for server authentication (unless all systems using the server are organization-managed, in which case a self-signed certificate could potentially be used instead)
□	For configurations that require a medium level of client authentication, configure server to require username and password via SSL/TLS
□	For configurations that require a high level of client authentication, configure server to require client certificates via SSL/TLS
□	Ensure weak cipher suites are disabled (see Table 7.1 for the recommended usage of Federal cipher suites)
□	Configure file integrity checker to monitor Web server certificate
□	If only SSL/TLS is to be used in the Web server, ensure access via any TCP port other than 443 is disabled
□	If most traffic to the Web server will be via encrypted SSL/TLS, ensure that appropriate logging and detection mechanisms are employed in the Web server (because network monitoring is ineffective against encrypted SSL/TLS sessions)

Completed	Action
	Protect against brute force attacks
□	Use strong authentication if possible
□	Use a delay after failed login attempts
□	Lock out an account after a set number of failed login attempts
□	Enforce a password policy
□	Blacklist IP addresses or domains known to attempt brute force attacks
□	Use log monitoring software to detect brute force attacks

Implementing a Secure Network Infrastructure

Completed	Action
	Identify network location
□	Web server is located in a DMZ, or Web server hosting is outsourced
	Assess firewall configuration
□	Web server is protected by a firewall; if it faces a higher threat or is more vulnerable, it is protected by an application layer firewall
□	Firewall controls all traffic between the Internet and the Web server
□	Firewall blocks all inbound traffic to the Web server except TCP ports 80 (HTTP) and/or 443 (HTTPS), if required
□	Firewall blocks (in conjunction with the IDPS) IP addresses or subnets that the IDPS reports are attacking the organizational network
□	Firewall notifies the network or Web server administrator of suspicious activity through an appropriate means
□	Firewall provides content filtering (application layer firewall)
□	Firewall is configured to protect against DoS attacks
□	Firewall detects malformed or known attack URL requests
□	Firewall logs critical events
□	Firewall and firewall OS are patched to latest or most secure level
	Evaluate intrusion detection and prevention systems
□	Host-based IDPS is used for Web servers that operate primarily using SSL/TLS
□	IDPS is configured to monitor network traffic to and from the Web server after firewall
□	IDPS is configured to monitor changes to critical files on Web server (host-based IDPS or file integrity checker)
□	IDPS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
□	IDPS notifies the IDPS administrators or Web server administrator of attacks through appropriate means
□	IDPS is configured to maximize detection with an acceptable level of false positives
□	IDPS is configured to log events
□	IDPS is updated with new attack signatures frequently (e.g., on a daily basis)
□	Host-based IDPS is configured to monitor the system resources available in the Web server host
	Assess network switches
□	Switches are used to protect against network eavesdropping

Completed	Action
□	Switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks
□	Switches are configured to send all traffic on network segment to network-based IDPS
	Evaluate load balancers
□	Load balancers are used to increase Web server availability
□	Load balancers are augmented by Web caches if applicable
	Evaluate reverse proxies
□	Reverse proxies are used as a security gateway to increase Web server availability
□	Reverse proxies are augmented with encryption acceleration, user authentication, and content filtering capabilities, if applicable

Administering the Web Server

Completed	Action
	Perform logging
□	Use the combined log format for storing the Transfer Log or manually configure the information described by the combined log format to be the standard format for the Transfer Log
□	Enable the Referrer Log or Agent Log if the combined log format is unavailable
□	Establish different log file names for different virtual Web sites that may be implemented as part of a single physical Web server
□	Use the remote user identity as specified in RFC 1413
□	Store logs on a separate (syslog) host
□	Ensure there is sufficient capacity for the logs
□	Archive logs according to organizational requirements
□	Review logs daily
□	Review logs weekly (for more long-term trends)
□	Use automated log file analysis tool(s)
	Perform Web server backups
□	Create a Web server backup policy
□	Back up Web server differentially or incrementally on a daily to weekly basis
□	Back up Web server fully on a weekly to monthly basis
□	Periodically archive backups
□	Maintain an authoritative copy of Web site(s)
	Recover from a compromise
□	Report the incident to the organization's computer incident response capability
□	Isolate the compromised system(s) or take other steps to contain the attack so additional information can be collected
□	Investigate similar hosts to determine if the attacker has also compromised other systems
□	Consult, as appropriate, with management, legal counsel, and law enforcement officials expeditiously
□	Analyze the intrusion
□	Restore the system

Completed	Action
□	Test system to ensure security
□	Reconnect system to network
□	Monitor system and network for signs that the attacker is attempting to access the system or network again
□	Document lessons learned
	Test security
□	Periodically conduct vulnerability scans on Web server, dynamically generated content, and supporting network
□	Update vulnerability scanner prior to testing
□	Correct any deficiencies identified by the vulnerability scanner
□	Conduct penetration testing on the Web server and the supporting network infrastructure
□	Correct deficiencies identified by penetration testing
	Conduct remote administration and content updates
□	Use a strong authentication mechanism (e.g., public/private key pair, two-factor authentication)
□	Restrict hosts that can be used to remotely administer or update content on the Web server by IP address and to the internal network
□	Use secure protocols (e.g., SSH, HTTPS)
□	Enforce the concept of least privilege on remote administration and content updating (e.g., attempt to minimize the access rights for the remote administration/update accounts)
□	Change any default accounts or passwords from the remote administration utility or application
□	Do not allow remote administration from the Internet unless mechanisms such as VPNs are used
□	Do not mount any file shares on the internal network from the Web server or vice versa

APPENDIX C: NIST SP800-44 CHECKLISTS (AGGREGATED BY CHECKLIST & CATEGORY)

Checklist 1 – Planning and Managing Web Servers	
Plan the configuration and deployment of the Web server	
	Identify functions of the Web server
	Identify categories of information that will be stored, processed, and transmitted through the Web server
	Identify security requirements of information
	Identify how information is published to the Web server
	Identify the security requirements of other hosts involved (e.g., backend database or Web service)
	Identify a dedicated host to run the Web server
	Identify network services that will be provided or supported by the Web server
	Identify the security requirements of any additional services provided or supported by the Web server
	Identify how the Web server will be managed
	Identify users and categories of users of the Web server and determine privilege for each category of user
	Identify user authentication methods for the Web server and how authentication data will be protected
	Identify how access to information resources will be enforced
	Identify appropriate physical security mechanisms
	Identify appropriate availability mechanisms
Choose appropriate OS for Web server	
	Minimal exposure to vulnerabilities
	Ability to restrict administrative or root level activities to authorized users only
	Ability to control access to data on the server
	Ability to disable unnecessary network services that may be built into the OS or server software
	Ability to control access to various forms of executable programs, such as CGI scripts and server plug-ins
	Ability to log appropriate server activities to detect intrusions and attempted intrusions
	Provision of a host-based firewall capability
	Availability of experienced staff to install, configure, secure, and maintain OS
Choose appropriate platform for Web server	
	General purpose OS
	Trusted OS
	Web server appliance
	Pre-hardened OS and Web server
	Virtualized platform
Checklist 2 - Securing the Web Server Operating System	
Patch and upgrade OS	
	Create, document, and implement a patching process

	Keep the servers disconnected from networks or on an isolated network that severely restricts communications until all patches have been installed
	Identify and install all necessary patches and upgrades to the OS
	Identify and install all necessary patches and upgrades to applications and services included with the OS
	Identify and mitigate any unpatched vulnerabilities
Remove or disable unnecessary services and applications	
	Disable or remove unnecessary services and applications
Configure OS user authentication	
	Remove or disable unneeded default accounts and groups
	Disable non-interactive accounts
	Create the user groups for the particular computer
	Create the user accounts for the particular computer
	Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)
	Prevent password guessing (e.g., increase the period between attempts, deny login after a defined number of failed attempts)
	Install and configure other security mechanisms to strengthen authentication
Configure resource controls appropriately	
	Deny read access to unnecessary files and directories
	Deny write access to unnecessary files and directories
	Limit the execution privilege of system tools to system administrators
Install and configure additional security controls	
	Select, install, and configure additional software to provide needed controls not included in the OS, such as antivirus software, antispyware software, rootkit detectors, host-based intrusion detection and prevention software, host-based firewalls, and patch management software
Test the security of the OS	
	Identify a separate identical system
	Test OS after initial install to determine vulnerabilities
	Test OS periodically (e.g., quarterly) to determine new vulnerabilities
Checklist 3 - Securing the Web Server	
Securely install the Web server	
	Install the Web server software on a dedicated host or a dedicated virtualized guest OS
	Apply any patches or upgrades to correct for known vulnerabilities
	Create a dedicated physical disk or logical partition (separate from OS and Web server application) for Web content
	Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, remote administration)
	Remove or disable all unneeded default login accounts created by the Web server installation
	Remove all manufacturer documentation from server
	Remove any example or test files from server, including scripts and executable code
	Apply appropriate security template or hardening script to the server
	Reconfigure HTTP service banner (and others as required) NOT to report Web server and OS type and version

Configure OS and Web server access controls	
	Configure the Web server process to run as a user with a strictly limited set of privileges
	Configure the Web server so that Web content files can be read but not written by service processes
	Configure the Web server so that service processes cannot write to the directories where public Web content is stored
	Configure the Web server so that only processes authorized for Web server administration can write Web content files
	Configure the host OS so that the Web server can write log files but not read them
	Configure the host OS so that temporary files created by the Web server application are restricted to a specified and appropriately protected subdirectory
	Configure the host OS so that access to any temporary files created by the Web server application is limited to the service processes that created the files
	Install Web content on a different hard drive or logical partition than the OS and Web server application
	If uploads are allowed to the Web server, configure it so that a limit is placed on the amount of hard drive space that is dedicated for this purpose; uploads should be placed on a separate partition
	Ensure that log files are stored in a location that is sized appropriately; log files should be placed on a separate partition
	Configure the maximum number of Web server processes and/or network connections that the Web server should allow
	Ensure that any virtualized guest OSs follow this checklist
	Ensure users and administrators are able to change passwords
	Disable users after a specified period of inactivity
	Ensure each user and administrator has a unique ID
Configure a secure Web content directory	
	Dedicate a single hard drive or logical partition for Web content and establish related subdirectories exclusively for Web server content files, including graphics but excluding scripts and other programs
	Define a single directory exclusively for all external scripts or programs executed as part of Web server content (e.g., CGI, ASP)
	Disable the execution of scripts that are not exclusively under the control of administrative accounts. This action is accomplished by creating and controlling access to a separate directory intended to contain authorized scripts
	Disable the use of hard or symbolic links (e.g., shortcuts for Windows)
	Define a complete Web content access matrix. Identify which folders and files within the Web server document should be restricted and which should be accessible (and by whom)
	Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)
	Use the robots.txt file, if appropriate
	Configure anti-spambot protection, if appropriate (e.g., CAPTCHAs, nofollow, or keyword filtering)
Checklist 4 - Securing Web Content	
Ensure that none of the following types of information are available on or through a public Web server	
	Classified records
	Internal personnel rules and procedures
	Sensitive or proprietary information

	Personal information about an organization's personnel
	Telephone numbers, e-mail addresses, or general listings of staff unless necessary to fulfill organizational requirements
	Schedules of organizational principals or their exact location (whether on or off the premises)
	Information on the composition, preparation, or optimal use of hazardous materials or toxins
	Sensitive information relating to homeland security
	Investigative records
	Financial records (beyond those already publicly available)
	Medical records
	Organization's physical and information security procedures
	Information about organization's network and information system infrastructure
	Information that specifies or implies physical security vulnerabilities
	Plans, maps, diagrams, aerial photographs, and architectural plans of organizational building, properties, or installations
	Copyrighted material without the written permission of the owner
	Privacy or security policies that indicate the types of security measures in place to the degree that they may be useful to an attacker
Establish an organizational-wide documented formal policy and process for approving public Web content that—(see items below)	
	Identifies information that should be published on the Web
	Identifies target audience
	Identifies possible negative ramifications of publishing the information
	Identifies who should be responsible for creating, publishing, and maintaining this particular information
	Provides guidelines on styles and formats appropriate for Web publishing
	Provides for appropriate review of the information for sensitivity and distribution/release controls (including the sensitivity of the information in aggregate)
	Determines the appropriate access and security controls
	Provides guidance on the information contained within the source code of the Web content
Maintain Web user privacy	
	Maintain a published privacy policy
	Prohibit the collection of personally identifying data without the explicit permission of the user and collect only the data that is absolutely needed
	Prohibit the use of "persistent" cookies
	Use the session cookie only if it is clearly identified in published privacy policy
Mitigate indirect attacks on content	
	Ensure users of the site are aware of the dangers of phishing and pharming attacks and how to avoid them
	Validate official communication by personalizing emails and providing unique identifying (but not confidential) information only the organization and user should know
	Use digital signatures on e-mail if appropriate
	Perform content validation within the Web application to prevent more sophisticated phishing attacks (e.g., cross-site scripting based attacks)
	Personalize Web content to aid in users' identifying fraudulent Web sites

	Use token-based or mutual authentication if applicable
	Suggest the use of Web browsers or browser toolbars with phishing/ pharming protection
	Use current versions of DNS software with the latest security patches
	Install server-side DNS protection mechanisms
	Monitor organizational domains and similar domains
	Simplify the structure of organization domain names
	Use secure connections for logins
	If necessary, engage a vendor to provide stronger anti-phishing/ anti-pharming measures
Client-side active content security considerations	
	Weigh the risks and benefits of client-side active content
	Take no actions without the express permission of user
	When possible, only use widely-adopted active content such as JavaScript, PDF, and Flash
	When possible, provide alternatives (e.g., HTML provided along with PDF)
Maintain server-side active content security	
	Only simple, easy-to-understand code should be used
	Limited or no reading or writing to the file system should be permitted
	Limited or no interaction with other programs (e.g., sendmail) should be permitted
	There should be no requirement to run with suid privileges on Unix or Linux
	Explicit path names should be used (i.e., does not rely on path variable)
	No directories have both write and execute permissions
	All executable files are placed in a dedicated folders
	SSIs are disabled or the execute function is disabled
	All user input is validated
	Web content generation code should be scanned or audited
	Dynamically created pages do not create dangerous metacharacters
	Character set encoding should be explicitly set in each page
	User data should be scanned to ensure it contains only expected input, (e.g., a-z, A-Z, 0-9); care should be taken with special characters or HTML tags
	Cookies should be examined for any special characters
	Encryption mechanism is used to encrypt passwords entered through scripts forms
	For Web applications that are restricted by username and password, none of the Web pages in the application should be accessible without executing the appropriate login process
	All sample scripts are removed
	No third-party scripts or executable code are used without verifying the source code
Checklist 5 - Using Authentication and Encryption Technologies for Web Servers	
Configure Web authentication and encryption technologies	
	For Web resources that require minimal protection and for which there is a small, clearly defined audience, configure address-based authentication
	For Web resources that require additional protection but for which there is a small, clearly defined audience, configure address-based authentication as a second line of defense
	For Web resources that require minimal protection but for which there is no clearly defined audience, configure basic or digest authentication (better)

	For Web resources that require protection from malicious bots, configure basic or digest authentication (better) or implement mitigation techniques discussed in Section 5.2.4
	For organizations required to comply with FIPS 140-2, ensure the SSL/TLS implementation is FIPS-validated
	For Web resources that require maximum protection, configure SSL/TLS
Configure SSL/TLS	
	Ensure the SSL/TLS implementation is fully patched
	Use a third-party issued certificate for server authentication (unless all systems using the server are organization-managed, in which case a self-signed certificate could potentially be used instead)
	For configurations that require a medium level of client authentication, configure server to require username and password via SSL/TLS
	For configurations that require a high level of client authentication, configure server to require client certificates via SSL/TLS
	Ensure weak cipher suites are disabled (see Table 7.1 for the recommended usage of Federal cipher suites)
	Configure file integrity checker to monitor Web server certificate
	If only SSL/TLS is to be used in the Web server, ensure access via any TCP port other than 443 is disabled
	If most traffic to the Web server will be via encrypted SSL/TLS, ensure that appropriate logging and detection mechanisms are employed in the Web server (because network monitoring is ineffective against encrypted SSL/TLS sessions)
Protect against brute force attacks	
	Use strong authentication if possible
	Use a delay after failed login attempts
	Lock out an account after a set number of failed login attempts
	Enforce a password policy
	Blacklist IP addresses or domains known to attempt brute force attacks
	Use log monitoring software to detect brute force attacks
Checklist 6 - Implementing a Secure Network Infrastructure	
Identify network location	
	Web server is located in a DMZ, or Web server hosting is outsourced
Assess firewall configuration	
	Web server is protected by a firewall; if it faces a higher threat or is more vulnerable, it is protected by an application layer firewall
	Firewall controls all traffic between the Internet and the Web server
	Firewall blocks all inbound traffic to the Web server except TCP ports 80 (HTTP) and/or 443 (HTTPS), if required
	Firewall blocks (in conjunction with the IDPS) IP addresses or subnets that the IDPS reports are attacking the organizational network
	Firewall notifies the network or Web server administrator of suspicious activity through an appropriate means
	Firewall provides content filtering (application layer firewall)
	Firewall is configured to protect against DoS attacks
	Firewall detects malformed or known attack URL requests
	Firewall logs critical events

	Firewall and firewall OS are patched to latest or most secure level
Evaluate intrusion detection and prevention systems	
	Host-based IDPS is used for Web servers that operate primarily using SSL/TLS
	IDPS is configured to monitor network traffic to and from the Web server after firewall
	IDPS is configured to monitor changes to critical files on Web server (host-based IDPS or file integrity checker)
	IDPS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
	IDPS notifies the IDPS administrators or Web server administrator of attacks through appropriate means
	IDPS is configured to maximize detection with an acceptable level of false positives
	IDPS is configured to log events
	IDPS is updated with new attack signatures frequently (e.g., on a daily basis)
	Host-based IDPS is configured to monitor the system resources available in the Web server host
Assess network switches	
	Switches are used to protect against network eavesdropping
	Switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks
	Switches are configured to send all traffic on network segment to network-based IDPS
Evaluate load balancers	
	Load balancers are used to increase Web server availability
	Load balancers are augmented by Web caches if applicable
Evaluate reverse proxies	
	Reverse proxies are used as a security gateway to increase Web server availability
	Reverse proxies are augmented with encryption acceleration, user authentication, and content filtering capabilities, if applicable
Checklist 7 - Administering the Web Server	
Perform logging	
	Use the combined log format for storing the Transfer Log or manually configure the information described by the combined log format to be the standard format for the Transfer Log
	Enable the Referrer Log or Agent Log if the combined log format is unavailable
	Establish different log file names for different virtual Web sites that may be implemented as part of a single physical Web server
	Use the remote user identity as specified in RFC 1413
	Store logs on a separate (syslog) host
	Ensure there is sufficient capacity for the logs
	Archive logs according to organizational requirements
	Review logs daily
	Review logs weekly (for more long-term trends)
	Use automated log file analysis tool(s)
Perform Web server backups	
	Create a Web server backup policy
	Back up Web server differentially or incrementally on a daily to weekly basis
	Back up Web server fully on a weekly to monthly basis

	Periodically archive backups
	Maintain an authoritative copy of Web site(s)
Recover from a compromise	
	Report the incident to the organization's computer incident response capability
	Isolate the compromised system(s) or take other steps to contain the attack so additional information can be collected
	Investigate similar hosts to determine if the attacker has also compromised other systems
	Consult, as appropriate, with management, legal counsel, and law enforcement officials expeditiously
	Analyze the intrusion
	Restore the system
	Test system to ensure security
	Reconnect system to network
	Monitor system and network for signs that the attacker is attempting to access the system or network again
	Document lessons learned
Test security	
	Periodically conduct vulnerability scans on Web server, dynamically generated content, and supporting network
	Update vulnerability scanner prior to testing
	Correct any deficiencies identified by the vulnerability scanner
	Conduct penetration testing on the Web server and the supporting network infrastructure
	Correct deficiencies identified by penetration testing
Conduct remote administration and content updates	
	Use a strong authentication mechanism (e.g., public/private key pair, two-factor authentication)
	Restrict hosts that can be used to remotely administer or update content on the Web server by IP address and to the internal network
	Use secure protocols (e.g., SSH, HTTPS)
	Enforce the concept of least privilege on remote administration and content updating (e.g., attempt to minimize the access rights for the remote administration/update accounts)
	Change any default accounts or passwords from the remote administration utility or application
	Do not allow remote administration from the Internet unless mechanisms such as VPNs are used
	Do not mount any file shares on the internal network from the Web server or vice versa